DOD ROLE FOR SECURING UNITED STATES CYBERSPACE

THESIS

Jane J. Griffin, GG-13, DAF

AFIT/GCO/ENG/08-03

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GCO/ENG/08-03

DOD ROLE FOR SECURING UNITED STATES CYBERSPACE

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science (Cyber Operations)

Jane J. Griffin, AAS, BS, MBA

GG-13, DAF

March 2008

AFIT/GCO/ENG/08-03

DOD ROLE FOR SECURING UNITED STATES CYBERSPACE

Jane J. Griffin, AAS, BS, MBA

GG-13, DAF

Approved:

//signed//	
Robert F. Mills, Ph.D. (Chairman)	Date
//signed//	
Richard A. Raines, Ph.D. (Member)	Date
//signed//	
Paul D. Williams, Ph.D. (Member)	Date

Abstract

The cyber attacks on Estonia in late April and the early weeks of May 2007 significantly crippled the country, preventing it from performing banking, communications, news reporting, government transactions and command and control activities. Estonia is considered a "Wired Society", much like the United States. Both countries rely on the cyberspace infrastructure economically and politically. Estonia sought assistance outside the country to recover from and to address the attacks. The cyber attacks on Estonia focused world-wide attention on the effects that cyberspace attacks could have on countries. If a cyber attack of national significance occurred against the United States, what would the United States do? The Department of Defense is responsible for protecting the nation and its geographical boundaries from attack, but what is DoD's role for securing the United States' cyberspace? Research was conducted by studying national orders, strategies, policies plans, and doctrine to determine DoD's role for securing the United States' cyberspace. Research revealed that DoD is assigned the lead role as Sector Specific Agency (SSA) for the Defense Industrial Base (DIB). As the lead SSA for the DIB, DoD's role for securing the United States' cyberspace is to identify, assess, and improve risk management of the critical infrastructure within the DIB. Our nation's defense and military strength rely on the DoD which in turn relies on the DIB to enable DoD to perform its mission. Participation by the DIB is on a voluntary basis, with DIB participants making the risk management calls and implementing the strategies that best fit their needs, which may not serve national security objectives.

Acknowledgments

I would like to express my sincere appreciation to my faculty advisor, Dr. Robert Mills, for his support and guidance during the course of my thesis effort. His shared wisdom, advice, patience and insight were greatly appreciated. I want to thank Mr. Robert Kaufman for sponsoring my research. I want to thank my National Air and Space Intelligence Center (NASIC) managers (Mr. Mokas, Captain Grafton, Major Carey, Major Fletcher, Mr. O'Brien and Colonel Kross) for endorsing me in the opportunity to attend AFIT full-time to complete an advanced degree in Cyber Operations. I want to thank my co-workers who have supported me in this endeavor by shouldering my work while I was away at school full-time. I want to thank Lieutenant Colonel Bailey, whose advice and encouragement kept me going through the darkest of times. I want to thank my husband for his patience and for understanding and supporting me in my educational goals as a non-traditional student. I want to thank my step-daughter, son-in-law and grandkids for understanding my limited involvement with their activities over the last 18 months. I want to thank my family and friends for their understanding and support, especially my mom and my mother-in-law, and my friends and neighbors.

Jane J. Griffin

Table of Contents

Page

List of Figures

Page

List of Tables

Page

DOD ROLE FOR SECURING UNITED STATES CYBERSPACE

I. Introduction

1.1. Motivation for Research

For several weeks in May 2007, it was widely reported in the news that cyber attacks were being committed against Estonia by creating a distributed denial-of-service (DDOS) on Estonia's national infrastructure (government, financial, and commercial websites) [1]. The attackers of Estonia's infrastructure used Botnets to perform the DDOS. Botnets are networks of remote-controlled zombie computers. The owners/users of these zombie computers are not aware that their computers are being used for these types of activities [2]. Estonia first realized it was under attack when government and banking transactions ceased to work globally within the country. One of Estonia's largest banks reported losses of at least $1 million dollars during the cyber attacks [3].

Estonia's defense minister, Mr. Jaak Aaviksoo, reported that more than 1 million computers worldwide had been used over several weeks to attack Estonian government and business Web site. At first, it appeared that Russia was behind the cyber attacks as several of the attacking Internet Protocol (IP) addresses were publicly identified as Russian government IP addresses, but later analysis did not bear this out. Estonia requested assistance from NATO, as these attacks could have been seen as an act of war, even though it was clear who was behind the attacks.

NATO sent several cyber experts to Estonia to assist in determining where the attacks originated and to further strengthen the cyber security procedures already in place. Analysis of these attacks categorized them as “cyber riots”. Eventually, the attacks were traced back to an Estonian student, and seven months later in January 2008, the 20-year-old Estonian hacker was fined approximately $1,620.00 for the cyber attack [4]. The scales of justice do not seem very equal when comparing the fine to the amount of losses incurred by just one of Estonia’s banks.

Now, substitute the United States for Estonia. The U.S. relies on information technologies from the simplest task of making a phone call using voice over internet protocol (VOIP) to deploying a weapon against an adversary. Today's interconnected systems and networks allow us to operate around the world through cyberspace within a matter of seconds exposing our infrastructure to cyberspace threats affecting our national security, public safety and personal privacy.

Table 1 provides the number of internet users and country population for Estonia [5] and the United States as of 30 November 2007 [6].

Table 1: Internet Statistics for Estonia and United States
(Source: Internet World Stats Usage and Population Statistics)

Country	Population	# Internet Users	% Users
United States (US)	301,139,947	215,088,545	71.4
Estonia (EE)	1,315,912	760,000	57.8

Comparing the number of cyber users between the two countries, the United States has nearly 300 times as many internet users as Estonia. While direct comparisons are difficult to make, it is clear that a similar type of cyber attack against the United States could affect significantly more people, impacting the safety, morale, and security

of our American citizens as well as our nation's economy. If the United States experienced cyber attacks of the same intensity as Estonia's, what role would DoD have in securing the United States' cyberspace from cyber attacks? How could we be sure who is attacking in a timely matter and the intent of the attack? In conventional warfare one can ascertain who performed the attack by examining the delivery method and materials in a timely matter. A cyber attack is more difficult to attribute, and the differences between warlike and criminal acts are blurred.

The threats still exist for an adversary to physically attack the United States, but a skilled cyberspace state or non-state adversary could strike at the heart of America's homeland remotely and anonymously. Our reliance on the power and capabilities of Information Technology (IT), which may contain vulnerabilities exploitable by an adversary, could ultimately be our weakness, our Achilles Heel.

> *"Today, the cyber economy is the economy. And I don't mean the dot coms. I mean virtually every vital service -- water supply, transportation, energy, banking and finance, telecommunications, public health. All of these rely upon computers and the fiber-optic lines, switches and routers that connect them. Corrupt those networks, and you disrupt the nation. It is a paradox of our times: the very technology that makes our economy so dynamic and our military forces so dominating -- also makes us more vulnerable. …. And everyday it is driven home to us that the threat is not just theoretical....Protecting our nation's critical infrastructure can only be done in concert with private industry"* [7].

The United States relies on cyberspace for the simplest of day-to-day activities to the most complex activities. Our national security, public health and safety, economic well-being, and way of life depend on the critical infrastructures and key resources being available to us in cyberspace. Our government and military rely on cyberspace to perform its missions. Our commerce relies on cyberspace to conduct its activities.

The typical citizen relies on cyberspace for day-to-day activities. With the advances in technology over the last twenty years, people can now perform video teleconferencing (VTC), make phone calls around the world and connect to local wireless networks available in various cities around the world. Our nation's citizens rely on cyberspace to pay bills, purchase merchandise, groceries, and fuel, buy and sell stocks, file government taxes online, manage financial accounts (savings, checking, loan application requests and repayment plans), participate in government elections, and communicate via email and Voice over IP (VOIP). Global Positioning Systems (GPS) provide highly accurate position, velocity, and time navigation information to users via cyberspace. Cyberspace supports transportation on the ground, in the air, on the water, under the water, and in space. Cyberspace is used to provide information to consumers, filter and provide the safe water that we consume on a daily basis, provide comfortable environments to work in, and defend our country against adversaries.

> "*Cyber is the United States' Center of Gravity--the hub of all power and movement, upon which everything else depends. It is the Nation's neural network"* [8].

1.2. Problem Statement

This research attempts to determine what role the DoD performs in securing the United States' homeland cyberspace. This paper explores the strategies and plans put in place to prevent a cyberspace attack from occurring against the United States' critical infrastructures and affecting the national security and safety. The research examines the government's chain of command to determine if clear lines of command are in place so that if a cyberspace attack occurred against the nation's critical infrastructures, someone

would be in charge and be able to direct actions from the "big picture" perspective, as well as provide information sharing with all the key players. The nation does not want a repeat of government failure to take action when a national disaster occurs such as the Hurricane Katrina in 2005.

Congress investigated the disastrous Hurricane Katrina incident that occurred in August 2005 and released a report titled "A Failure of Initiative" which detailed the lack of actions by top level government managers to address a national crisis. That report sited numerous problem areas throughout the federal and state governments. One major finding was that "Communications between DOD and DHS, and in particularly FEMA, during the immediate week after landfall, reflect a lack of information sharing, near panic, and problems with process" [9].

1.3. Research Questions

This research will first explore the DoD's role for securing the United States' homeland. This will be done by analyzing the strategic and national policies and legal authorities. Next the research answers the question of what is DoD's role for securing the United States' cyberspace. To answer this question, the research uses the following investigative questions:

- What is DoD's role for securing the United States homeland critical infrastructure from cyber attack?
- What support can DoD provide to civil authorities to respond and recover from cyber attack?
- Can/should the National Guard and reserve members' roles be expanded to support cyberspace roles and functions?

The research first studies the laws, national strategies, policies, plans and guidelines that are in place for DoD to secure the United States. The research then explores DoD's role for securing the United States' cyberspace, how DoD can work with other agencies to respond to and recover from cyberspace attacks, and the feasibility of expanding the National Guard and reserve members roles for performing cyberspace functions.

1.4. Scope

The scope for this thesis is centered on the DoD role, without special regard to a specific branch of service. Branches of service may be mentioned, but only to support a point being made in the research paper. The research also focuses on national cyberspace defense and not offensive or expeditionary operations.

1.5. Methodology

The research will consist of referencing the types of documents, web resources, and training materials associated with securing the United States' cyberspace. A content analysis and a critical review of published national and strategic policies and guidance directives will be performed for tracing DoD's responsibilities to defend the United States homeland and secure the United States' cyberspace. This research will attempt to determine if adequate plans are in place for DoD to secure the United States' cyberspace. Based on the findings, it will make recommendations to prevent a "cyberspace Hurricane Katrina" from occurring.

Throughout the research effort, many definitions of cyberspace were found. This research uses the official DoD definition: "*Cyberspace is a domain characterized by the*

use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated infrastructures" [10].

1.6. Limitations

The time limit for completing this thesis was based on a six-month window out of an 18 month program. Additional limitations for this thesis are, that during the course of this research and before being published, new laws, guidelines, policies may be put into place, causing some of the research and conclusions to be overcome by events. The information presented in this thesis is publicly available; however, due to the nature of the Cyber Storm exercise, some of the exercise results may be withheld from the public due to national security.

1.7. Research Outline

Chapter I provides the background for this thesis. It covers the need for this type of research, the problem statement, the research objectives, the scope, methodology, and limitations of this research.

Chapter II provides a literature review of national laws, strategies, directives and plans guiding the DoD and the Department of Homeland Security (DHS) for defending the United States' cyberspace.

Chapter III examines more closely the literature providing guidance to the DoD and DHS organizations. It explores the research and investigative questions to determine if documentation exists to address DoD's role for securing the United States' cyberspace. If the documentation exists, this chapter provides the answers to the research and investigative questions.

Chapter IV examines the answers to the research and investigative questions for strengths and weaknesses and provides a gap analysis with recommendations for addressing perceived deficiencies.

Chapter V provides the conclusions based on the research findings and includes recommendations for future research.

Appendix A provides an Acronym List, and Appendix B provides a list of Terms and Definitions.

II. Literature review

2.1. Introduction

This chapter summarizes the literature reviewed to answer the research and investigative questions. The methodology used to identify the documents for literature review consisted of researching areas that related to cyberspace, DoD roles, homeland defense and security, and critical infrastructures. It is important to understand what national security is before delving into the national orders, strategies, directives and plans. This chapter defines national security and then discusses the national orders, strategies, directives and plans pertinent to the problem of securing and defending the nation's cyberspace information infrastructure. It provides a summary of the purpose for each order, strategy, directive and plan, detailing who generated the document, when it was generated, and why it was generated. These documents will be reviewed and discussed in more detail in Chapter III, as needed. A summary of the literature review is provided at the end of this chapter.

2.2. National Security

> *"If the attacking side secretly...launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hack detachment in the opponent's computer system in the advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis"* [11].

National security is about protecting the sovereignty of our nation, defending our borders, and promoting and embracing our American way of life. This includes protecting our nation from attack whether from other nation states or non-nation states and defeating our adversaries, if required and protecting our way of life. Our nation leverages its instruments of national power--Diplomatic, Information, Military and Economic (DIME) to wield influence and promote our national security interests.

The National Security Act of 1947 provided a comprehensive program for the security of the United States by establishing the National Security Council; Secretary of Defense; a National Military Establishment; Departments of the Army, Navy, and Air Force; and coordination of the activities of the National Military Establishment with other departments and agencies of the Government concerned with the national security [12].

The following sections examine the national strategies, directives, plans and orders that provide guidance to our great nation, concentrating on critical infrastructure and cyberspace.

2.3. National Orders, Strategies, Directives and Plans

Following the terrorist attacks on the United States on 11 September 2001 (9/11), executive orders, national strategies, directives and plans were issued for protecting the nation's homeland and critical infrastructure. This section presents these orders, strategies, directives and plans in the chronological timeline that they were issued in order to assist the reader in following the history of securing the nation's homeland and its cyberspace infrastructure. Executive orders and national strategies provide the

guidance for leveraging our nation's instruments of national power (DIME). The National Security Strategy (NSS) provides the overarching strategy for guiding our nation. The National Defense Strategy (NDS) defines strategic objectives to support the NSS and provides the high-level guidance for development of the National Military Strategy (NMS). The NMS defines national military objectives based on the NSS, NDS, and the current security environment. DoD Directives provide guidance to DoD organizations for performing their assigned duties and responsibilities. National plans provide guidance for securing and responding to incidents of national significance.

An outline of these orders, national strategies, directives and plans are listed below.

Executive Order 13231 - Critical Infrastructure Protection in the Information Age

Executive Order (EO) 13231- Critical Infrastructure Protection in the Information Age, issued by the White House on Oct 16, 2001, provided the policy for protecting the information systems for the nations' critical infrastructures [13]. This order updated the United States Code Title 50 – War and National Defense. USC Title 50 created the National Defense Council for coordination of industries and resources for the nation's security and well-being [14].

National Strategy for Homeland Security

The National Strategy for Homeland Security, issued by the White House in July 2002, is the first Homeland Security document to be released [15]. It complemented the National Security Strategy of the United States by addressing terrorism within the United

States. The National Strategy for Homeland Security establishes the foundation for organizing the nation's efforts to secure the US homeland from terrorist attack. It also provides initial guidance on how to achieve this goal.

Homeland Security Act of 2002

The Homeland Security Act of 2002, issued on 25 November 2002, established the Department of Homeland Security (DHS) and defined its mission [16]. United States Code (USC) Title 6 – Domestic Security is also referred to as the Homeland Security Act 2002.

Homeland Security Presidential Directive/HSPD-5

HSPD-5, Management of Domestic Incidents, issued by the White House on 28 February 2003, assigned the Secretary of Defense Homeland Security as the lead federal official for coordinating resources and responding to homeland incidents generated by terrorist attacks, major disasters and other types of emergencies [17]. HSPD-5 established the National Incident Management Systems (NIMS) to provide a consistent nationwide approach for Federal, state and local governments to work together to prepare for and respond to and recover from domestic incidents.

National Strategy to Secure Cyberspace

The National Strategy to Secure Cyberspace, issued in February 2003 by the White House [18], is an implementing component of the National Strategy for Homeland Security [19] and is complemented by The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets [20]. The National Strategy to Secure

Cyberspace encourages Americans to secure the portions of cyberspace that they own, operate, control, or interact with. The government cannot do it alone.

National Strategy for the Physical Protection of CI and Key Assets

The National Strategy for the Physical Protection of Critical Infrastructures (CI) and Key Assets, issued in February 2003 by the White House, identifies the national goals and outlines guiding principles to secure the nation's critical infrastructures and key assets [20]. This strategy complements the National Strategy to Secure Cyberspace.

Homeland Security Presidential Directive/HSPD-7

HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, issued 17 December 2003, established national policy for identifying and prioritizing US critical infrastructures and key resources and protecting them [21]. HSPD-7 identified the roles and responsibilities for Secretary of Department of Homeland Security and also documented DoD as the sector-specific lead agency for the Defense Industrial Base.

The National Military Strategy of the United States of America

The National Military Strategy (NMS) of the United States of America, issued in 2004, derives its objectives from the NSS, NDS and the current security environment [22]. The current security environment consists of four types of challenges: (1) Traditional: state employs recognized military capabilities; (2) Irregular: Use of unconventional methods to counter stronger opponent; (3) Catastrophic: Use of Weapons of Mass Destruction or producing WMD-like effects; and (4) Disruptive: Use of technology to affect Critical Infrastructure and Key Resources (CI/KR): for example – a

cyberspace attack. NMS states its three military objects as: (1) Protect the United States against external attacks and aggression; (2) Prevent conflict and surprise attack; and (3) Prevail against adversaries. Preventing conflict and surprise cyber attacks address the disruptive challenges of our nation's current security environment.

National Response Plan

The National Response Plan, issued by DHS in December 2004, establishes a comprehensive, national, all-hazards approach to domestic incident management [23]. It includes prevention, preparedness, response and recovery guidance, for responding to attacks, disasters, and other emergencies of national significance. Incident annexes are provided for responding to Biological, Catastrophic, Cyber, Food and Agriculture, Nuclear and Radiological, Oil and Hazardous Materials, and Terrorism Incident Law Enforcement and Investigation events. The Cyber Incident Annex provides the framework for responding to cyber incidents of national significance.

The National Defense Strategy of the United States of America

The National Defense Strategy (NDS) of the United States of America, issued by DoD in March 2005, states the Department of Defense's four strategic objectives for supporting the United States' National Security Strategy as: (1) Secure the United States from Direct Attack; (2) Secure Strategic Access and Retain Global Freedom of Action; (3) Strengthen Alliances and Partnerships; and (4) Establish Favorable Security Conditions [24]. The NDS provides high-level guidance for development of the National Military Strategy. Establishing favorable security conditions includes securing

cyberspace, and making it less vulnerable to exploits by adversaries. The NDS advocates using an active layered defense in protecting the United States' national security.

Strategy for Homeland Defense and Civil Support

The Strategy for Homeland Defense and Civil Support, issued by DoD in June 2005, supports guidance from the National Security Strategy, the National Defense Strategy, and the National Strategy for Homeland Security [25]. It performs the following activities to secure the United States from direct attack:

- Lead – At National Command Authority (NCA) direction, execute military missions to deter, dissuade, and defeat attacks on our nation, population, defense critical infrastructure
- Support – At NCA direction, provide support to civil authorities
- Enable – Share expertise and technology with military & civilian entities

DoD Directive 3020.40 Defense Critical Infrastructure Program (DCIP)

DoD Directive 3020.40, Defense Critical Infrastructure Program, issued in August 2005, implements Homeland Security Presidential Directive 7 (HSPD-7) to function as the Sector Specific Agency (SSA) for the Defense Industrial Base (DIB) [26]. The Director of the Defense Contract Management Agency (DCMA) is assigned the lead agent role for the DIB. The DoD, as the lead SSA for the DIB critical infrastructure sector, has the responsibilities to collaborate with all relevant departments, agencies, and private sector entities, conduct or facilitate vulnerability assessments of the sector, and encourage risk management strategies to protect and mitigate attack effects.

The National Security Strategy of the United States of America

> *"There was a time when two oceans seemed to provide protection from problems in other lands, leaving America to lead by example alone. That time has long since passed. America cannot know peace, security, and prosperity by retreating from the world. America must lead by deed as well as by example. This is how we plan to lead, and this is the legacy we will leave to those who follow"* [27:49].

The National Security Strategy (NSS) of the United States of America is updated as needed and was last released in March 2006 by the White House. It emphasizes making the world a safer better place, promoting activities for developing relationships with allies, partners, and friends, and documents the need for securing and against preventing attacks on the United States, and to work with other organizations and nations for providing a more secure environment for all to flourish and prosper [27:1-3].

National Infrastructure Protection Plan

DHS published the National Infrastructure Protection Plan (NIPP) in 2006 based on the requirements in the Homeland Security Presidential Directive 7 (HSPD-7) [28]. The NIPP provides the unifying structure for integrating CI/KR protection into a single national program. HSPD-7 designated various Sector Specific Agencies (SSAs) for DHS to coordinate with for the nation's Critical Infrastructure and Key Resources (CIKR).

Defense Industrial Base: Critical Infrastructure and Key Resources SSP

The Defense Industrial Base: Critical Infrastructure and Key Resources Sector Specific Plan, issued by DoD and DHS in May 2007, implements HSPD-7 direction for DoD to serve as lead Sector Specific Agency (SSA) for the Defense Industrial Base (DIB) [29]. As the lead SSA for the DIB, the DoD works closely with the DIB members

to identify critical assets, assess risk, and improve the sector's risk management posture. This SSP defines the DIB as

> "*The Department of Defense, U.S. Government, and private sector worldwide industrial complex with capabilities to perform research and develop, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements necessary to fulfill the National Military Strategy (NMS). The DIB is comprised of hundreds of thousands of industrial sites. The preponderance of the DIB is privately owned and comprised of businesses of all sizes*" [29:5].

2.4. Summary

This chapter provided a literature review and introduction of the national orders, strategies, directives, and plans that apply to securing and defending the United States critical infrastructures in cyberspace.

Chapter III examines the research methodology used to answer our research and investigative questions and delves more deeply into those documents that provide the answers to our research and investigative questions.

III. Methodology

3.1. Chapter Overview

The purpose of this chapter is to focus on the way in which the research was conducted. The literature review served as the foundation for this thesis, highlighting the key documents studied.

The research methodology consisted of the following activities:

- Reviewed the DoD and DHS organization structure
- Identified literature relevant to this research by performing searches of these related terms: “cyberspace, cyber war, cyber attack, homeland security, homeland defense, United States cyberspace, DoD role”, which led to perform further document searches on “national strategy, national security, national defense, and defense industrial base”
- Reduced the amount of identified relevant literature for this research to the subset identified in Chapter II
- Applied knowledge gained from AFIT graduate studies
- Traced DoD guidance for securing United States cyberspace through the national orders, strategies, directives and plans.
- Use identified literature to answer research and investigative questions
- Introduced reports on nation’s cyberspace exercise and DoD status of its risk management methodology for DIB critical infrastructure

This research examines the DoD’s chain of command and discusses the high-level DoD components. The research then examines the DHS’s organization structure, with regards to protection of the nation’s cyberspace infrastructure. Next the research utilizes the research and investigative questions to examine the documents identified in the literature review in Chapter II. The research explores the research question regarding the

DoD's role for securing the United States' cyberspace, using the following investigative questions:

- What is DoD's role for securing the United States' homeland from cyber attack?
- What support can DoD provide to civil authorities to respond and recover from cyber attack?
- Can/should the National Guard and reserve roles be expanded to support cyberspace roles and functions?

3.2. Department of Defense (DoD)

DoD's role for defending the United States is two-fold: 1) Provide the military forces to deter war; and 2) Protect the security of the United States. The literature review in Chapter II described the national security, defense and military strategies that provide the guidance to DoD for performing its mission. Traditionally, the DoD has achieved its mission by force or threat of force (deterrence) and projecting its power abroad.

The DoD's mission and functions are documented in Joint Publication 1 (JP1) Doctrine for the Armed Forces of the United States and are listed below:

> *"As prescribed by higher authority, the DOD will maintain and employ Armed Forces to fulfill the following aims: defend the Constitution of the United States (U.S.) against all enemies, foreign and domestic; ensure, by timely and effective military action, the security of the United States, its possessions and areas vital to its interest; and uphold and advance the national policies and interests of the United States. These functions are performed under the authority, direction, and control of the Secretary of Defense, who in turn reports to the President of the U.S., our Commander-in-Chief"* [30].

The President of the United States enforces the nation's laws and serves as Commander-in-Chief over the Armed Forces. The President and Secretary of Defense (referred to as National Command Authority (NCA) [30]) exercise authority and control

of the Armed Forces through two distinct branches of the chain of command as illustrated in Figure 1.

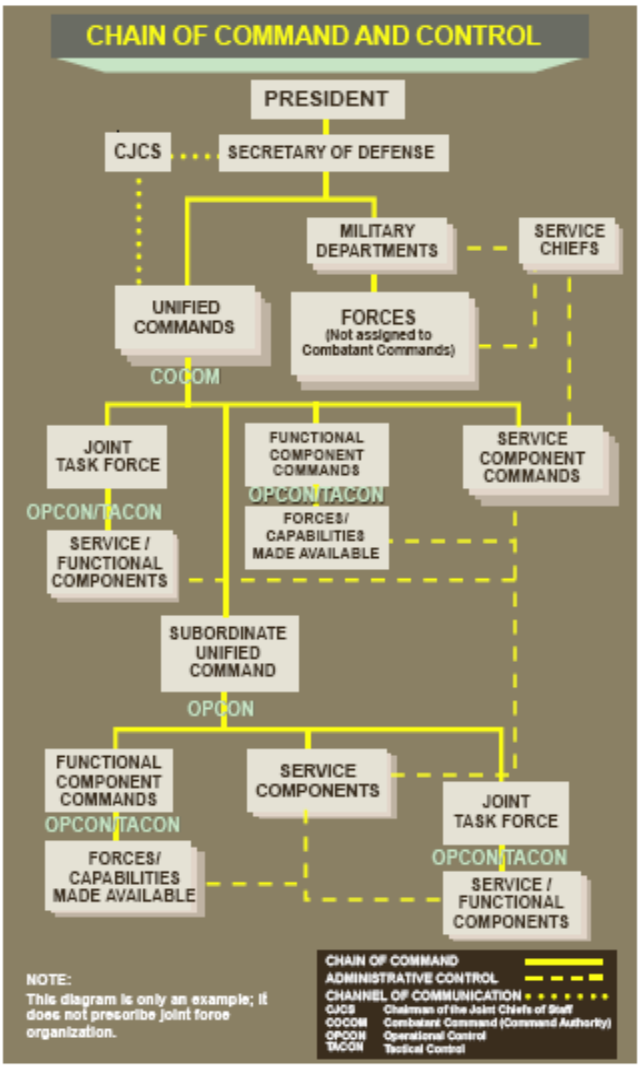

Figure 1. DoD Chain of Command and Control
[30:II-5]

In Figure 1, DoD Chain of Command and Control, the primary chain of command and control branch runs from the President through the Secretary of Defense (SECDEF) to the Unified Commands. The Unified Commands conduct military operations (in

peace-time and conflict) to support national objectives. There are a total of nine Unified Commands (UCs):

- United States Central Command (USCENTCOM) *
- United States Europe Command (USEUCOM) *
- United States Pacific Command (USPACOM) *
- United States Northern Command (USNORTHCOM) *
- United States Southern Command (USSOUTHCOM) *
- United States Strategic Command (USSTRATCOM)
- United States Transportation Command (USTRANSCOM)
- United States Special Operations Command (USSOCOM)
- United States Joint Forces Command (USJFCOM)

The five UCs listed above with "*" following their names have geographic Areas of Responsibility (AORs). The remaining UCs provide capabilities on a global scale or based on function. Figure 2 depicts these AORs.

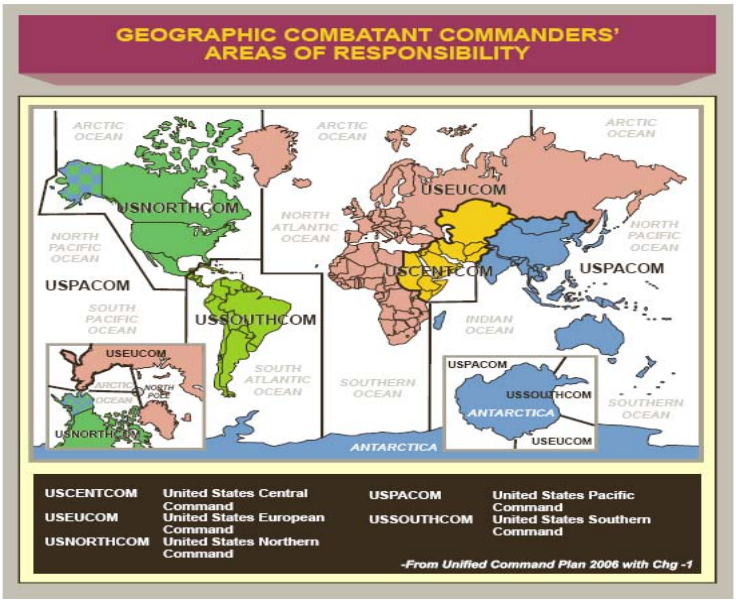

Figure 2: Combatant Commanders Geographic Areas of Responsibility (AORs) [31]

The second chain of command and control shown in Figure 1 is administrative in nature and is used for purposes other than operational direction of forces assigned to the

combatant commands. This branch runs from the President through the SECDEF to the Secretaries of the Military Departments.

The President is the ultimate authority as commander-in-chief of the armed forces. The Secretary of Defense tasks the Military Departments, Unified Commands, and the Chairman of Joint Chiefs of Staff for conducting the nation's military operations and executing national defense strategies.

The Military Departments (Air Force, Army and Navy) operate under the authority, direction, and control of the Secretary of each department. The primary mission of the Military Departments is to organize, train and equip forces to provide capabilities when needed in support of Combatant Commander (CCDR) requirements. The Secretaries exercise authority through their respective Service Chiefs over Service forces not directly assigned to the Unified Commands. The Service Chiefs, except as otherwise prescribed by law, perform their duties under the authority, direction, and control of the Secretaries of the respective Military Departments to whom they are directly responsible. Service Chiefs are senior military advisers to the National Command Authority (NCA) for matters pertaining to their respective service.

3.3. Department of Homeland Security (DHS)

The Department of Homeland Security's role is to lead the United States in unifying internal efforts to secure the vast national network of organizations and institutions involved in contributing to the economic well being and security of our country. Figure 3 illustrates the DHS organization chart.

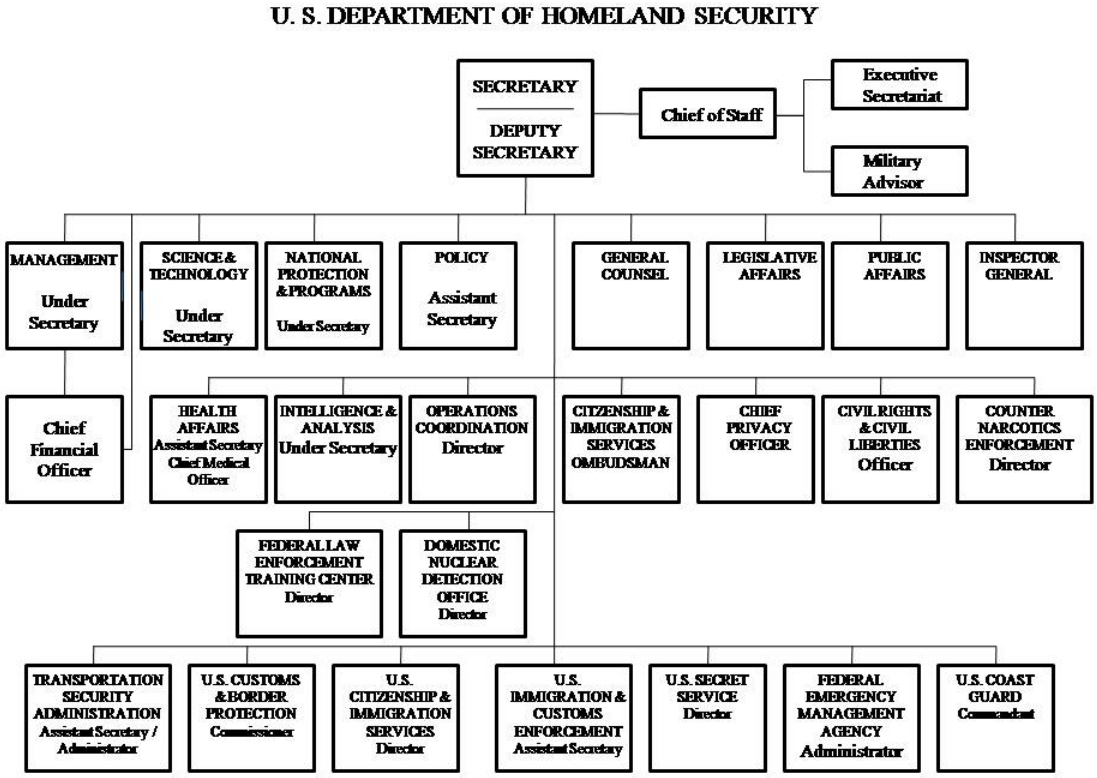

Figure 3: DHS Org Chart
[32:1]

The DHS is responsible for protecting the nation's "critical infrastructure" and key resources. The term "critical infrastructure" is defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Public Law 107-56, 115 Stat. 272, dated 26 October 2001, as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [33].

There are 25 offices reporting to Secretary of Homeland Security that are responsible for performing homeland security activities. Cyberspace security homeland defense activities are located in the National Protection & Programs Directorate (NPPD). The NPPD's mission is to promote the DHS's risk-reduction mission. Figure 4 illustrates the NPPD organization chart. The Infrastructure Protection office is responsible for ensuring that the nation's critical infrastructure and key resources are protected. The DoD SSA for the Defense Industrial Base works with the Infrastructure Protection Assistant Secretary under the National Protection & Programs office.

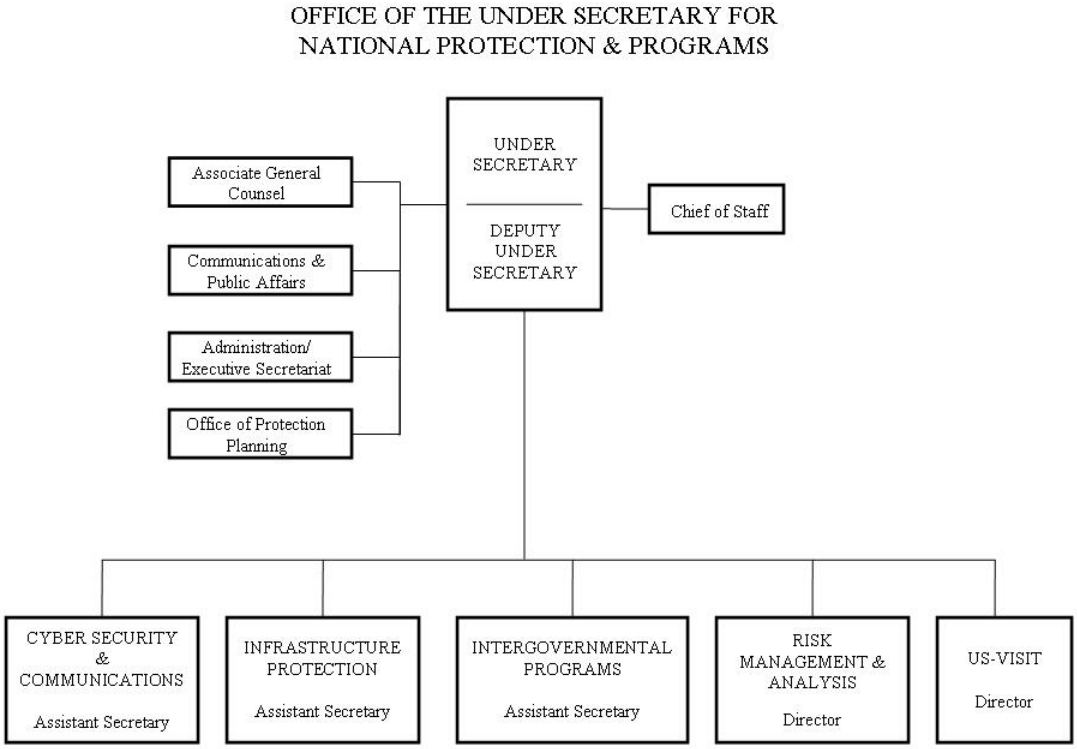

Figure 4: DHS National Protection and Programs Organization Chart
[32:11]

3.4. Literature Review Content Analysis

This section investigates the documents described in Chapter II in more detail. The research and investigative questions are used to guide the research.

What is DoD's role for securing the United States' cyberspace?

Examining the documents provided in the literature review, the research reveals that EO 13231 provides policy for protecting the information systems of our nation's critical infrastructures [13]. The National Strategy for Homeland Security provides guidance for securing the nation by integrating the capabilities of local, Tribal, State, and Federal governments with the private and non-profit sectors, in order to secure the critical infrastructures and key resources in the land, water, air, space, and cyber domains [15].

Securing the nation's homeland cannot be performed by government alone. Eight-five percent of the US infrastructure is privately owned [15]. It requires our entire society to get involved: the American people, federal, state, and local governments, and the private sector businesses. Homeland Security defines "State" as "*any state of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the trust territory of the Pacific Islands"* and defines "local government" as "*any county, city, village, town, district, or other political subdivision of any state, any Native American tribe or authorized tribal organization, or Alaska native village or organization, and includes any rural community or unincorporated town or village or any other public entity for which an application for assistance is made by a state or political subdivision thereof*" [15].

The National Strategy for Homeland Security defines the following six critical mission areas: intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response. The Protecting Critical Infrastructure and Key Assets (CI/KR) critical mission area contains the Securing of cyberspace initiative. The nation's critical infrastructures are complex and if successfully attacked, the effects from the attack could have far reaching damaging ripple effects throughout the infrastructure.

The National Strategy to Secure Cyberspace encourages Americans to secure the portions of cyberspace that they own, operate, control, or interact with and identified the lead SSAs for each of the critical infrastructures. The DoD is identified as the lead SSA for the DIB [15]. This strategy provides direction for empowering and engaging people in protecting the cyber domain under their jurisdiction. As is the case for the homeland in general, the government cannot defend cyberspace alone:

> *"The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace. The National Strategy to Secure Cyberspace provides a framework for protecting this infrastructure that is essential to our economy, security, and way of life… Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people"* [34].

Protecting the Nation's cyberspace domain involves effort from local, Tribal, State, and Federal governments, the private and non-profit sectors, and the American people. Figure 5 illustrates the roles and responsibilities of the American people in

securing cyberspace and the five national priorities for securing cyberspace. National Priority 1 focuses on improving our ability to respond to cyber incidents and reducing the potential damage from such incidents. National Priorities 2, 3, and 4 are aimed at reducing the number of exploitable vulnerabilities thus preventing successful cyber attacks, and National Priority 5 seeks to prevent cyber attacks that could affect national security assets such as the DoD, DIB, nation's cyberspace, and the nation's critical infrastructures. DoD, working with intelligence and law enforcement agencies, is tasked to attribute cyberspace attacks to ensure timely and appropriate responses to attacks.

Roles and Responsibilities in Securing Cyberspace					
	National Priority 1	National Priority 2	National Priority 3	National Priority 4	National Priority 5
	National Cyberspace Security Response System	National Cyberspace Security Threat and Vulnerability Reduction System	National Cyberspace Security Awareness and Training Program	Securing Governments' Cyberspace	National Security and International Cyberspace Security Cooperation
Home User/ Small Business		X	X		
Large Enterprises	X	X	X	X	X
Critical Sectors/ Infrastructures	X	X	X	X	X
National Issues and Vulnerabilties	X	X	X	X	
Global					X

Figure 5: Cyberspace Roles and Responsibilities
[18]

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets provides the guiding principles for securing the critical infrastructure and

addresses the protection challenge for each of the sectors. Figure 6 illustrates the DoD DIB protection challenge: ~ 250,000 firms in 215 distinct industries located worldwide.

THE PROTECTION CHALLENGE	
Agriculture and Food	1,912,000 farms; 87,000 food-processing plants
Water	1,800 federal reservoirs; 1,600 municipal waste water facilities
Public Health	5,800 registered hospitals
Emergency Services	87,00 U.S. localities
Defense Industrial Base	250,000 firms in 215 distinct industries
Telecommunications	2 billion miles of cable
Energy	
Electricity	2,800 power plants
Oil and Natural Gas	300,000 producing sites
Transportation	
Aviation	5,000 public airports
Passenger Rail and Railroads	120,000 miles of major railroads
Highways, Trucking, and Busing	590,000 highway bridges
Pipelines	2 million miles of pipelines
Maritime	300 inland/costal ports
Mass Transit	500 major urban public transit operators
Banking and Finance	26,600 FDIC insured institutions
Chemical Industry and Hazardous Materials	66,000 chemical plants
Postal and Shipping	137 million delivery sites
Key Assets	
National Monuments and Icons	5,800 historic buildings
Nuclear Power Plants	104 commercial nuclear power plants
Dams	80,000 dams
Government Facilities	3,000 government owned/operated facilities
Commercial Assets	460 skyscrapers
	*These are approximate figures.

Figure 6: United States' Protection Challenge
[20]

DoD cannot execute its mission without support of the Defense Industrial Base (DIB). The DIB provides most of the equipment, materials, services, and weapons used by DoD to perform its mission as defined by the national orders, strategies, directives and plans.

The National Military Strategy (NMS) of the United States of America derives its objectives from the NSS, NDS and the current security environment [22]. The Armed Forces provide homeland defense by securing strategic air, land, sea, and space access points to the United States and its territories. The Armed Forces task is to fight and win wars, defeating a wide range of adversaries from state to non-state entities. The Armed Forces must be prepared to address the following types of security environment challenges: (1) Traditional: state employs recognized military capabilities; (2) Irregular: Use of unconventional methods to counter stronger opponent; (3) Catastrophic: Use of Weapons of Mass Destruction or producing WMD-like effects; and (4) Disruptive: Use of technology to affect Critical Infrastructure and Key Resources (CI/KR): for example – a cyberspace attack.

The National Response Plan (NRP) for responding to incidents of national significance contains an annex for responding to cyber incidents [23]. The National Response Plan's Cyber Incident Annex "*discusses policies, organization, actions, and responsibilities for a coordinated, multidisciplinary, broad-based approach to prepare for, respond to, and recover from cyber-related Incidents of National Significance impacting critical national processes and the national economy*" [35].

As stated in the NRP Cyber Incident Annex, DoD's core roles and responsibilities for securing the nation's cyberspace and coordinating incident response are: 1) providing defense support to civil authorities; 2) providing intelligence and information-sharing; 3) assisting with law enforcement investigations; and 4) providing military operations to defend the homeland. This annex also stated: "*If authorized by applicable law and*

policy, DoD can take action to deter or defend against cyber attacks that pose a threat to our national security" [35]. The Cyber Incident Annex was exercised in February 2006 (known as exercise Cyber Storm), with results published in August 2006. The results of this report will be discussed in more detail in Chapter IV.

In the NRP's Cyber Incident Annex, DoD provides cyberspace support to DHS using the Joint Task Force – Global Network Operations (JTF-GNO) Computer Emergency Response Teams (CERT) to identify, mitigate, and if necessary, respond to cyber attacks. The U.S. Strategic Command (USSTRATCOM) and JTF-GNO provide intelligence analysis of cyber attacks. JTF-GNO also houses the Law Enforcement/Counter Intelligence Center which brings together DoD law enforcement and the counterintelligence organizations during a cyber incident.

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for integrating CI/KR protection into a single national program. The overarching goal of the NIPP is to:

> *"Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency*" [28].

Figure 7 demonstrates the NIPP CI/KR protection methodology scheme: manage the risks by deterring the threats, mitigating the vulnerabilities, or minimizing the consequences associated with a terrorist attack or other incident.

Figure 7: NIPP CI/KR Protection Methodology Model
[28]

There are seventeen critical infrastructures identified in the NIPP; all of them rely on cyberspace to be operational. Each Sector Specific Agency (SSA) works closely with DHS to develop Sector Specific Plans (SSPs) and with their respective sector specific partners to develop risk management and protective programs.

Figure 8 illustrates the United States' Critical Infrastructure / Key Resources (CI/KR) Sectors. Looking at this breakdown of SSAs, it appears that the SSA lead agencies are selected based on the critical infrastructure sectors that fall within their purview. It is up to each lead sector agency to coordinate within the sector and with other sectors that may have overlapping areas dependent on each other. As noted earlier, the DoD has been designated as the lead SSA for the DIB. DoD provided an annual SSP to DHS in May 2007.

Sector-Specific Agency (SSA)	Critical Infrastructure/Key Resources Sector
Department of Agriculture[1] Department of Health and Human Services[2]	Agriculture and Food
Department of Defense[3]	Defense Industrial Base
Department of Energy	Energy[4]
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems
Department of Homeland Security Office of Infrastructure Protection Office of Cyber Security and Telecommunications Transportation Security Administration Transportation Security Administration, United States Coast Guard[5] Immigration and Customs Enforcement, Federal Protective Service	 Chemical Commercial Facilities Dams Emergency Services Commercial Nuclear Reactors, Materials, and Waste Information Technology Telecommunications Postal and Shipping Transportation Systems[6] Government Facilities

1 The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).
2 The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.
3 Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DOD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.
4 The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.
5 The U.S. Coast Guard is the SSA for the maritime transportation mode.
6 As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

Figure 8: United States' Critical Infrastructure/Key Resources Sector

[28]

The Defense Industrial Base (DIB) Critical Infrastructure and Key Resources (CI/KR) Sector Specific Plan (SSP) provides a coordinated strategy for managing risk within DIB critical asset locations throughout the world and describes a risk management

approach and plan for the DIB. DoD relies on the DIB to provide the capabilities to support and sustain DoD accomplishing its mission. The absence or unavailability of some assets designated as critical DIB assets, and the products and services these assets produce, could cause military mission failure. The next two tables identify the products and services that DIB provides to DoD.

Table 2 lists the segment and sub-segment capabilities provided by the Defense Industrial Base to DoD.

Table 2: DIB Segments and Sub-segments
[29]

Segments	Sub-segments	Segments	Sub-segments
Missile	• Tactical Missile • Torpedo • Strategic Missile	Ammunition	• Bombs & Warheads • Cartridges & Fuses • Explosives
Aircraft	• Fixed Wing • Helicopter • Unmanned Aerial Vehicle	Weapons	• Small • Medium • Large
Troop Support	• Soldier Systems • Clothing & Textile • Subsistence/Medical • Smoke Obscurant • Nuclear, Biological, Chemical Systems	Information Technology	• Command, Control, Computers, & Intelligence • Information Security • Trainers & Simulators • Computer Peripherals
Space	• Launch Vehicle • Satellite	Shipbuilding	• Surface Ship • Subsurface
Combat Vehicle	• Tracked vehicle • Tactical vehicle	Electronics	• Electronic Warfare • SONAR • Radar

Table 3 lists the commodities capabilities provided by the Defense Industrial Base to DoD.

Table 3: DIB Commodities
[29]

Mechanical		
• Diesel Engines	• Automotive Transmission	• Nuclear Components
• Rocket Engines	• Landing Gear	• Hydraulics
• Turbine Engines	• Bearings	
• Aircraft Transmission	• Pumps & Compressors	
Structural		
• Forgings	• Depleted Uranium Armor	• Composites
• Castings	• Ceramic Armor	• Precious Metals
Electrical		
• Electrical Motors	• Auxiliary Power Units	• Aircraft Circuit Breakers
• Batteries Thermal	• Low Smoke Wire & Cable	• Switch Gear
Electronics		
• Optics	• Digitization	• Traveling Wave Tubes
• Guidance/Control	• GPS Receiver	• Circuit Boards
• Communication	• Semiconductors	• Software

As the lead SSA for the DIB, DoD's goals for protecting the Defense Industrial Base are: 1) Prevent/Delay an incident; 2) Detect a potential incident; 3) Mitigate/respond to incident; 4) Recover from an incident; and 5) Develop resiliency. [29:24]

The Defense Industrial Base (DIB) Critical Infrastructure and Key Resources (CI/KR) Sector Specific Plan (SSP) focuses on steps to 1) Identify a critical asset list by identifying Assets, Systems, networks and Functions; 2) Assess the risk based on mission, human, economic and public confidence impacts, consequences, vulnerabilities, and threats, 3) Prioritize the critical assets on that list; 4) Perform vulnerability assessments on high-priority critical assets; and 5) Encourage contractors' actions to remediate or mitigate adverse effects found during these assessments, as appropriate, to ensure continuity of business operations.

DoD generated the DoD Directive 3020.40 titled Defense Critical Infrastructure Program (DCIP) [26]. DoD assigned the Defense Contract Management Agency (DCMA) as the operational lead for the DCIP as DCMA manages government contracts with the DIB. DoD and DCMA focused their DCIP efforts on identifying and prioritizing assets, systems, networks, and functions that, if damaged, would result in unacceptable consequences to the DOD mission, national economic security, public health and safety, or public confidence.

Achieving the Mission Assurance objective (ability to mobilize, deploy and sustain U. S. military operations) requires having the core capabilities in place so that DoD can perform its assigned duties based on having access to the defense critical infrastructure. The defense critical infrastructure is defined as "*DoD and non-DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide*" [25]. Achieving the Mission Assurance objective requires ensuring the preparedness of the Defense Industrial base (DIB) and may also require DoD to protect DIB elements. The Defense Industrial Base is defined as "*DoD, the U.S. Government, and the private sector worldwide industrial complex with capabilities to perform research and development (R&D), design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements*" [29].

The Government Accountability Office (GAO) provided a report to Congress in August 2007 titled "Defense Infrastructure: Management Actions Needed to Ensure

Effectiveness of DOD's Risk Management Approach for the Defense Industrial Base" [36], which documented deficiencies in the DoD's DIB Risk Management Approach.

Table 4, Summary of DoD's Efforts in Identifying and Assessing Critical DIB Assets, provides the metrics for the current number of important and critical DIB assets identified and the number of contractors assessed as of 1 June 2007.

Table 4: Summary of DOD's Efforts in Identifying and Assessing Critical DIB Assets [36:12]

		Critical Contractors		
DIB Assets	Important	Domestic	Foreign	Total
Identified	900	194	9	203
Assessed*		8	0	8

*The number of contractors assessed does not include 5 that were completed prior to DCMA's pilot program being established

Table 5, Assessments Planned during Fiscal years 2007 to 2012, provides the projected metrics for performing DIB Critical Infrastructure Planning Mission Assurance Assessments (CIP MAA) on identified DIB assets.

Table 5: Assessments Planned during Fiscal Years 2007 to 2012 [36:16]

Fiscal year	2007	2008	2009	2010	2011	2012
Assessments Planned as of Nov 2006	19	50	50	50	20	20
Revised plan as of May 2007**	14	21	21	50	50	50

**DCMA is planning that after completing the initial assessments, DIB assets would be reassessed every three years

DoD issued the Strategy for Homeland Defense and Civil Support in June 2005 and is based on the National Defense Strategy's active layered defense concept.

"Homeland defense is the protection of US sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President [25]. DoD can provide civil assistance to

local government under the Posse Comitatus Act if authorized by the National Command Authority. The Posse Comitatus Act, 18 June 1878, limits DoD's capabilities for providing military assistance to domestic law enforcement. *"Unless under authorization by the President, Congress, or the Constitution, Posse Comitatus, together with related DOD regulations, prohibits the Army, Air Force, Marine Corps, and Navy from directly participating in civilian law enforcement activities within the United States*" [30]. The Strategy for Homeland Defense and Civil Support improves the nation's ability to respond to threats against the nation's homeland [25].

Figure 9 illustrates the strategy foundations for formulating DoD's Strategy for Homeland Defense and Civil Support.

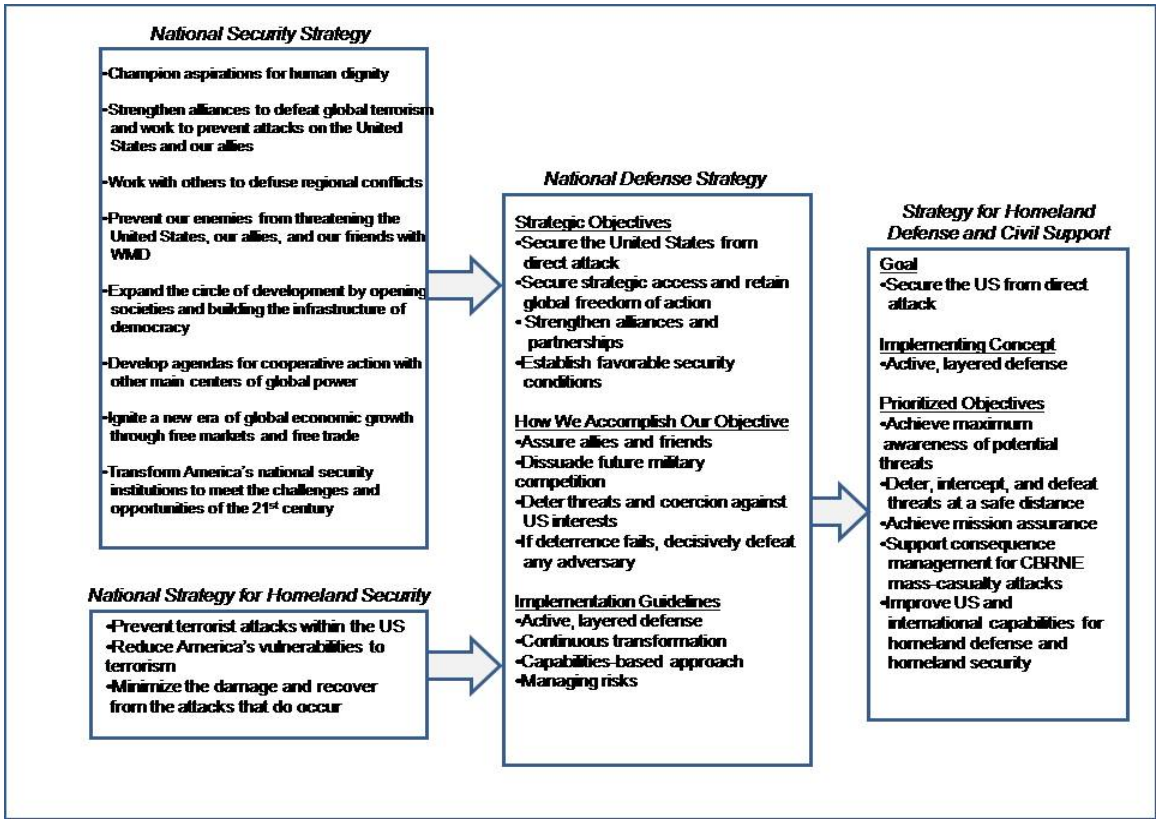

Figure 9: Foundations for DoD Strategy for Homeland Defense and Civil Support [25]

The National Security Strategy and National Strategy for Homeland Security provide guidance to the National Defense Strategy for defining its strategic objectives. The National Defense Strategy provides the guidance to the Strategy for Homeland Defense and Civil Support for securing the United States from direct attack.

Figure 10 illustrates DoD's Strategic Goals, Key Objectives, and its core capabilities for US Homeland Defense and Civil Support. DoD leads military missions to prevent, deter, and defeat attacks on the United States. DoD, when directed by NCA, provides defense support of civil authorities. DoD enables others by sharing capabilities and expertise with domestic agencies and international partners.

ACTIVITIES	*OBJECTIVES*	*CORE CAPABILITIES*
LEAD	Achieve Maximum Awareness of Threats	- Maintain agile and capable defense intelligence architecture - Analyze and understand potential threats - Detect, identify, and track emerging threats in all operational domains - Ensure shared situational awareness within DoD and with domestic and foreign partners
	Deter, Intercept, and Defeat Threats at a Safe Distance	- Deter adversaries from attacking the US homeland - Intercept and defeat national security threats in the maritime and air approaches and within US territory
	Achieve Mission Assurance	- Ensure force protection, to include DoD installations, especially against the threat of CBRNE attacks - Prepare and protect defense critical infrastructure - Ensure preparedness of the Defense Industrial Base - Prepare to protect designated national critical infrastructure - Ensure DoD crisis management and continuity preparedness
SUPPORT	Support Consequence Management for CRBNE Mass Casualty Attacks	- Manage consequences of CBRNE mass casualty attacks
ENABLE	Improve National and International Capabilities for Homeland Defense and Homeland Security	- Effective interagency planning and interoperability - Improved Federal, state, and local partnership capacity and effective domestic relationships - Improved international partnership capacity and effective defense-to-defense relationships

Figure 10: DoD Objectives and Core Capabilities for Protecting the US from Attack [25]

The Strategy for Homeland Defense and Civil Support designates USNORTHCOM, USPACOM, and USSTRATCOM as being responsible for defending the nation's homeland cyberspace infrastructure and providing civil support.

USNORTHCOM and USPACOM conduct operations for addressing threats against the United States, their geographic AOR territories and their AORs' interests. They are also tasked to provide military assistance to civil authorities when directed by the National Command Authority under the Posse Comitatus Act [37]. They will respond to civil support incidents when the local and state support agencies are unable to deal with the incidents [25]. The other regional combatant commanders have a lesser role in defending the nation's homeland cyberspace since they are responsible for maintaining their own networks within their AOR.

USSTRATCOM's mission objectives are: 1) Provide the nation with global deterrence capabilities; 2) Synchronize DoD effects to combat adversary weapons of mass destruction worldwide; 3) Enable decisive global kinetic and non-kinetic combat effects through the application and advocacy of integrated intelligence, surveillance and reconnaissance (ISR); 4) Provide space and global strike operations; 5) Information Operations (IO); and 6) Integrated missile defense and robust command and control [38].

One of USSTRATCOM's component commands is the Joint Task Force – Global Network Operations (JTF-GNO) command. JTF-GNO is responsible for assuring system and network availability, information protection, and timely information delivery using the Global Information Grid (GIG) across the strategic, operational, and tactical boundaries in support of DoD's mission [39]. USSTRATCOM also contains the Joint

Functional Component Command – Network Warfare (JFCC-NW) which "facilitates cooperative engagement with other national entities in computer network defense and network warfare as part of the global information operations mission." [40]

National Guard and Reserve members can be activated to serve as regular armed forces by presidential order under United States Code Title 10 – Armed Forces. USC Title 10 – Armed Forces defines the United States military organization and its powers [41]. USC Title 10, Subtitle A, Part I, Chapter 18 Military Support for Civilian Law Enforcement Agencies provides the legal guidance for providing Armed Forces to assist federal, state, and local law enforcement agencies.

National Guard forces can also be activated by a state governor to serve in time of a state emergency. USC Title 32 – National Guard defines the United States National Guard and its powers. Title 32, Chapter 9 (Homeland Defense Activities) provides the legal guidance for providing National Guard to assist in homeland defense activities [42].

The Defense Contract Management Agency (DCMA) is using National Guard and Reserve Forces to perform the Critical Infrastructure Protection – Mission Assurance Assessments (CIP-MAAs) of the DIB sector for performing the DoD Directive 3020.40, Defense Critical Infrastructure Program (DCIP).

The DoD role for securing the United States' cyberspace is to serve as the lead SSA for protecting the Defense Industrial Base (DIB) critical infrastructure using risk management methodology. DoD provides homeland defense and civil support if authorized by the National Command Authority (NCA). DoD responds to cyber attacks

in coordination with DHS and other agencies if the cyber attacks are deemed of national significance and authorized by law and policy.

When reviewing DoD as a role model for DIB cyber security practices, one has only to read the latest news reports to determine that DoD has its own problems in securing its infrastructure from cyberspace attacks. Andrew Palowitch, a former CIA official and industry consultant to the USSTRATCOM Commander stated, "America is under widespread attack in cyberspace," and cited "statistics that there were 37,000 reported breaches of government and private systems in fiscal 2007. There were nearly 13,000 direct assaults on federal agencies then, and 80,000 attempted computer network attacks on Defense Department systems … Some of those assaults reduced the U.S., military operational capabilities" [43].

In The National Security Strategy of the United States of America, President Bush reflected that *"This strategy reflects our most solemn obligation: to protect the security of the American people"* [27]. This strategy is based on two pillars. The first pillar promotes freedom, democracy, justice, human dignity, and prosperity through free and fair trade. The second pillar is confronting the challenges of our time by leading world-wide efforts to address the challenges. The challenges of our time include addressing disruptive security environment challenges where technology is used to affect our nation's critical infrastructure and key resources (CI/KR). DoD's goals for defending the DIB critical infrastructure include addressing the disruptive security environment challenges.

3.5. Investigative Questions

Now that the research has reviewed the literature from Chapter II and answered the research question, the research moves to the investigative questions and answers them with the gained knowledge from reviewing the literature and answering the research question.

What is DoD's role for securing the United States homeland critical infrastructure from cyber attack?

In the National Strategy for Homeland Security, the National Strategy to Secure Cyberspace and the National Infrastructure Protection Plan, DoD is identified as the lead Sector Specific Agency for the securing the United States cyberspace for the Defense Industrial Base critical infrastructure.

In the National Response Plan's Cyber Incident Annex, DoD entities responsible for computer security and computer network defense may provide defense support of civil authorities, provide information sharing and intelligence, assist in law-enforcement investigations, and provide military operations to defend the homeland. DoD can take action to deter or defend against cyber attacks that pose a threat to our national security, if authorized by the applicable law and policy [35]. All cyber attacks against the nation's critical infrastructures/key resources that have national significance, affect the national security of the American people, and NCA authority to respond, can cause DoD to engage. The nation's cyberspace is under attacks around the clock, but these attacks typically do not require DoD intervention.

One type of cyber attack could include obvious attempts to affect the well-being of the United States in cyberspace. It could be as devastating as producing major electrical outages with cascading effects preventing people from purchasing the basic necessities (food & water) to lack of communications to American people. Major electrical outages could create chaos, and DoD could be called upon to assist in providing civil support to local law enforcement agencies. Additionally, DoD could assist in determining attribution for the attack, and if ordered by the National Command Authority, could take action against the United States space cyber attacker. Effects from this type of United States cyberspace attack could ripple to the Defense Industrial Base, preventing it from providing capabilities to DoD consisting of: missiles, aircraft, troop support, space capabilities, combat vehicles, ammunition, weapons, information technology, shipbuilding, electronics, and mechanical, structural, electrical, and electronic parts. By not having these capabilities provided by the Defense Industrial Base, DoD cannot achieve its mission. These capabilities provide DoD with the products and services necessary to equip, inform, mobilize, deploy, and sustain operations worldwide.

When the terrorist physical attacks on the United States occurred on 11 September 2001 (9/11), it was nationally devastating. In addition to the physical destruction, there was a severe psychological impact. People wanted to know how this could happen to our great country. Our nation's people experienced a great deal of concern over just being able to get food, water and purchasing of fuel for their vehicles. Rumors were being passed around that our water supplies and oil refineries were going to be attacked. The

airline industry was in shock. The New York Stock Exchange was non-operational for approximately one week, affecting our nation's prosperity and economic well-being. People were afraid to attend major events that may be targeted by terrorists. The DoD provided civil support and military support for homeland defense during the aftermath of the 9/11 incident. This attack forced the nation to look at its own infrastructures and identify those critical infrastructures that were critical to the nation's well-being. The DIB was identified as a critical infrastructure and DoD was assigned to protect it as the lead SSA.

What support can DoD provide to Civil Authorities to respond and recover from cyber attack?

In the National Strategy to Secure Cyberspace, DoD, law enforcement agencies, and the Intelligence Community (IC) are tasked with improving the attack prevention and attack attribution capabilities. In the National Response Plan's Cyber Incident Annex, DoD can take action to deter or defend against cyber attacks that pose a threat to our national security, if authorized by the applicable law and policy [35]. DoD was designated as the lead agency for the Defense Industrial Base. DoD works with over 250,000 firms in 215 distinct industries located worldwide to protect the Defense Industrial Base (DIB). DoD supports the DIB in reducing risks from cyber attacks or hazards by using these goals as their guideline: 1) Preventing/Delaying an incident; 2) Detecting a potential incident; 3) Mitigating/Responding to incident; 4) Recovering from Incident; and 5) Developing resiliency. The USNORTHCOM and USPACOM can provide the appropriate DoD personnel to assist civil authorities in addressing the cyber

attacks. The DIB critical infrastructures are responsible for their own recovery using Contingency Plans, Continuity of Operations, and relying on Backups.

Can/Should the National Guard and reserve members' roles be expanded to support cyberspace roles and functions?

The National Guard and reserve members can be used and are being used by DoD in supporting DoD's role as the lead sector-specific agency (SSA) for the Defense Industrial Base Critical Infrastructure and Key Resource (CI/KR). National Guard personnel are providing Critical Infrastructure Protection (CIP) Mission Assurance Assessment (MAA) training for individuals who perform DIB assessments. National Guard personnel are also performing the CIP-MAA at various DIB sites [44].

3.6. Summary

This chapter presented the methodologies used in the research to perform literature review and content analysis of literature relevant to this research.

Cyberspace has existed in our work environments for over fifty years, however, only through technological advances have we been able to integrate cyberspace into our daily lives. The last twenty years have seen the release of the first piece of malware software in 1988 known as the internet worm (which was fairly harmless) to more recent events of cyber attacks being committed on the country of Estonia [45].

Protecting the Nation's cyberspace domain involves effort from local, Tribal, State, and Federal governments, the private and non-profit sectors, and the American people.

> *"And so, my fellow Americans: ask not what your country can do for you--ask what you can do for your country."*
>
> (Source: Inaugural Address of President John F. Kennedy)

John F. Kennedy spoke the above words during his inaugural speech on 20 January 1961 [46]. These words apply almost fifty years later to our effort to defend and protect US cyberspace critical infrastructure. Americans can take these words to heart and do their part in securing cyberspace (keeping their systems patched and virus signatures up to date are just a few ways). We must all do our part to keep America's cyberspace safe.

DoD's role in defending the United States' cyberspace is diversified by serving as the lead sector-specific agency (SSA) for the Defense Industrial Base (DIB). The DIB consists of over 250,000 firms for 215 unique industries required to support the DoD in accomplishing its mission. As the lead SSA for the DIB, DoD works with the DIB in performing risk management.

In Chapter IV, the research examines the results of the literature review and contents analysis and looks more closely at some of the results the review provided. In particular, the research is looking more closely at the GAO Audit report of DoD and the DIB and the Cyber Storm exercise results.

IV. Results and Analysis

4.1. Chapter Overview

Chapter III reviewed and analyzed the literature focusing on the research and investigative questions. It also introduced two additional documents generated by GAO and the DHS for providing insight into how DoD is performing in securing the DIB critical infrastructure cyberspace and for detailing the Cyber Storm Exercise performed by DHS with its critical infrastructure lead SSAs, private sector representatives, emergency responders, and some of our nation's international partners.

In this chapter, the research examines the recommendations and findings in the GAO report titled: "Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DoD's Risk Management Approach for the Defense Industrial Base", published August 2007 and in the DHS Cyber Storm exercise report, published September 2006. The research analyzes the findings and makes observations. The research then summarizes the findings at the end of this chapter.

4.2. GAO report on DOD Risk Management Approach for DIB Analysis

The GAO report titled: "Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DoD's Risk Management Approach for the Defense Industrial Base" identified the following summarized findings [36:26]:

- DOD is not including the military services' listings of assets whose damage, degradation, or destruction would result in DOD-wide mission failure
- DoD cannot be sure it has identified the most important and critical assets, as called for in the National Military Strategy. This finding is based on how the

weighting factors were selected and data determined according to subjective decisions and limited review, and that needed contractor-specific data were lacking, as was comprehensive threat information, thus undermining the utility of the index score for prioritizing contractors.

- Scheduling and conducting assessments of critical DIB assets without regard for assets' priority rankings

- DoD lacks a plan for working with the Department of State and other appropriate agencies to identify and address potential challenges in assessing vulnerabilities in foreign critical DIB assets

DoD's challenge for the Defense Industrial Base is to prioritize DIB assets based on criticality and put processes in place to protect its cyberspace infrastructure [47]. Cyberspace is vulnerable to attacks by anyone having access to a computer with network connectivity using tools available for free on the internet [48]. To prevent successful cyberspace attacks, one must implement cyber security layers in place to protect the data and maintain information superiority. Cyber security layers include protecting the confidentiality, integrity, and the availability (CIA) of information, authentication, implementing access controls and monitoring, auditing and logging of security events, implementing intrusion detection and virus scanning systems, and maintaining system backups critical data. The CIA Triad is only good if all three legs are secure. If any of the legs fail, then the information owner is susceptible to cyberspace attacks. In order to maintain Information superiority, one must be able to maintain three CIA Triad legs [49].

Sophisticated attackers can intercept information, change the content, and pass the modified information off as being authentic, affecting the integrity leg of the CIA Triad. Sophisticated attackers can monitor information being passed in clear text and gather information about its target, breaking the CIA Triad leg for confidentiality. Sophisticated

attackers can perform distributed denial of service (DDOS) attacks, flooding a target's systems with meaningless message traffic and making the target's systems unavailable, affecting the availability leg of the CIA Triad. The methods listed above are just a few examples of how the CIA Triad can be broken.

The National Strategy to Secure Cyberspace assigned DoD's role for defending the United States' cyberspace to serve as the lead Sector Specific Agency (SSA) for protecting the nation's critical infrastructure asset's Defense Industrial Base [18]. DoD published the DoD Directive 3020.40 (DoD, 2005) [27] incorporating the President's guidance issued in Homeland Security Presidential Directive #7 (HSPD-7) [22] to serve as the Sector-Specific Agency (SSA) for the Defense Industrial Base. DoD Directive 3020.40 states the following:

- Collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector.
- Conduct or facilitate vulnerability assessments of the sector.
- Encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

An old proverb states that "a chain is only as strong as its weakest link". In this sense, the "chain" terminology is used to represent the nation's cyberspace critical infrastructures. The Defense Industrial Base consists of over 250,000 firms spread over 215 unique industries around the world. Cyber infrastructure security is typically left up to the private sector, with voluntary participation in vulnerability assessments [50].

DIB companies want to be competitive in the market, sometimes taking shortcuts to get a product or service to the market before their competitor beats them out. All of

this is done at what cost? Typically, cyber security is added as an after-thought unless the contract specifically states cyber security is required. Companies have contractual and legal obligations to its customers, its shareholders, and to its governing body. In the midst of delivering products and services on-time and within budget, and following all mandated laws and guidelines, it is easy to forget about the non-mandated efforts, such as voluntary assessments of critical infrastructures. Program managers juggle schedules all the time and experience information overload trying to get the products and services delivered on time and within budget.

Sixty years ago, Dr. Norbert Weiner published the paper “Cybernetics: or Control and Communication in the Animal and the Machine” [51] in October 1948, and was considered by the American Scientist magazine at the turn of the century among the most “memorable and influential” works of the twentieth century. He authored this paper after working for the United States on developing an automated anti-aircraft system for the United States, developing communications theory, leading to the development of the term “cybernetics”. Dr. Wiener defined cybernetics as "the science of control and communication in the animal and the machine”. In his paper, he predicted “information overload” conditions caused by an excess amount of traffic [52]. 60 years later, we are still concerned with “information overload” conditions. Information overload can prevent individuals from making good decisions and from maintaining information superiority. Performing Risk Management with the DIB provides information overload conditions for the DCMA and assessment teams as the DIB consists of more than

215,000 companies scattered around the world, with DIB members having unique characteristics.

4.3. DHS Cyber Storm Exercise Analysis

Homeland Security Presidential Directive #5 (HSPD-5) [17] directed the creation of the National Response Plan (NRP) [23] to establish the framework for the United States to manage domestic incidents. The NRP's objective is to improve coordination among Federal, State, Local and tribal organizations for saving lives and protecting the nation.

The NRP contains the Cyber Incident Annex that is executed when a cyber attack occurs against the United States' national infrastructure that could threaten the lives, property, the nation's economy or national security [35]. The NRP Cyber Incident Annex states the following DoD roles and responsibilities for securing cyberspace and coordinating incident responses: 1) Defense Support of Civil Authorities; 2) intelligence and information-sharing; 3) law enforcement investigations; and 4) military operations to defend the homeland. If authorized by applicable law and policy, DOD can take action to deter or defend against cyber attacks which pose an imminent threat to national security.

The Department of Homeland Security' (DHS) National Cyber Security Division (NCSD) executed the NRP's first Cyber Incident Annex on 6-10 February 2006 and published its findings on 12 September 2006 [53]. This exercise was titled Cyber Storm and included over 100 public and private agencies, associations, and corporations from over 60 locations and 5 countries, over 30 private sector corporations, along with designated Federal and State governments.

The Cyber Storm exercise simulated a large-scale cyber attack affecting multiple critical infrastructures within the Energy, IT, Transportation, and Telecommunications sectors. There were 8 significant findings resulting from the exercise:

- Interagency coordination needed to be refined such that the cyber community better understood when to activate federal engagement
- Contingency Planning, Risk Assessment, and Roles and Responsibilities needed to be solidified
- Correlation of Multiple Incidents Between Public and Private Sectors remained a challenge
- Training and Exercise Program needed to be established and executed to ensure everyone knew the roles, policies, and procedures
- Coordination Between Entities of Cyber Incidents was challenged as the number of incidents increased
- Common Framework for Response and Information Access strengthened information sharing between domestic and international cyber response communities
- Strategic Communications and Public Relations Plan must be part of the collaborated contingency plan
- Improvement of Processes, Tools, and Technology required to enhance the quality, speed and coordination of response

DHS, NCSD, and exercise participants incorporated lessons learned from the Cyber Storm 2006 exercise findings. Plans are in place for the next exercise titled Cyber Storm II to occur in March 2008 [54]. It will be interesting to see the results of this next exercise.

It is not clear from analyzing the report findings if the cyber exercise progressed to the point of authorizing by applicable law and policy DoD to take action to deter or

defend against the cyber attacks which posed an imminent threat to national security. If this happened, it was not detailed in the findings. It is critical to detail the procedure for determining when to engage DoD to deter or defend against cyber attacks which pose an imminent threat to national security, and the unity of command for performing this.

The type of Cyber attack that will impact DoD can be compared to results of the September 11, 2001 physical attack on the United States' homeland which shut down all air and train transportation until security procedures could be put in place to monitor passengers, shut down the New York Stock Exchange for approximately five business days, and greatly impacted the Manhattan's business district [55].

It can also be compared to the effects of the natural disaster Hurricane Katrina in August 2005 which affected the United States' Gulf coast states and rippled throughout the country causing gas prices to go up, among other things. The government was not at its best performance when the "failure to initiate" occurred for Hurricane Katrina causing lives to be lost, failures in communications and the lack of following procedures to get the assistance from the federal government that the gulf coast states needed. The gulf coast states are still reeling (over two years later) from the effects of the hurricane, but are slowly coming back to life [56]

DoD's Strategy for Homeland Defense and Civil Support (SHDCS) provides the guidance for DoD in performing Homeland Defense and Civil Support [25]. The Assistant Secretary of Defense for Homeland Defense is in charge of DoD's homeland defense activities. US Northern Command (USNORTHCOM) is responsible for planning, organizing, and executing homeland defense and civil support missions within

the continental United States, Alaska, and territorial waters. US Pacific Command (USPACOM) has homeland defense and civil support responsibilities for Hawaii and US territories, possessions and freely associated states.

If directed by the President or the SECDEF of the United States, DoD can provide assistance to local law enforcement agencies, provide intelligence and information-sharing to assist in characterizing the cyber attack and attributing the attack to an entity, assist in law enforcement operations, and perform military operations to defend the homeland. DoD can take actions to deter or defend against cyber attacks which pose an imminent threat to national security based on applicable laws and policies.

The National Guard's role in providing cyber support to Civil Authorities consists of supporting DoD's Critical Infrastructure Protection (CIP) role for performing CIP Mission Assurance Assessments (MAA) on the Defense Industrial base (DIB) components [57]. The DoD DCIP has collaborated with the National Guard Bureau, the Defense Contract Management Agency (DCMA), the West Virginia National Guard, the Naval Surface Warfare Center's (NSWC) Mission Assurance Division to develop CIP-MAA curriculum for training DIB assessment personnel. The DIB is cooperating with the National Guard members for assessing their operations.

4.4. Summary

DoD's role in defending the United States' cyberspace is diversified by serving as the lead sector-specific agency (SSA) for the Defense Industrial Base (DIB). The DIB consists of over 250,000 firms for 215 unique industries required to support the DoD in accomplishing its mission. GAO published findings of its assessment for DoD in

performing risk management of the DIB and DHS published findings from its cyber exercise. It is clear from reviewing these findings that there is still much work to be done by DoD in securing the nation's critical infrastructures.

V. Conclusion

5.1. Discussion

The DoD role for securing the United States cyberspace is serving as the lead Sector Specific Agency (SSA) for protecting the Defense Industrial Base (DIB) critical infrastructure's cyberspace. DoD can provide homeland defense and civil support if directed by National Command Authority, and can respond to cyber attacks of national significance if authorized to do so, coordinating response with DHS and other agencies. DoD can encourage and sometimes mandate to the DIB sector (based on the national security level of the DIB's role) best practices in cyber security. However, DoD cannot defend DIB's cyberspace on its own. Each of the DIB partners must take an active role in securing its own cyberspace.

Potential adversaries are aware that the United States' relies heavily on the cyberspace infrastructure to perform its DoD mission at home and abroad [58]. These adversaries are studying the types of cyberspace information systems and vulnerabilities associated with them that are being used by the US. United States' cyberspace is under constant surveillance, with malicious actors hoping to find weaknesses that can be exploited for gaining information superiority over our nation.

The DoD published DoD Directive 3020.40 (DoD, 2005) [26] incorporating the President's guidance issued in Homeland Security Presidential Directive 7 (HSPD-7) [21] to serve as the Sector-Specific Agency (SSA) for the Defense Industrial Base.

The Directive states that DoD will do the following:

- Collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector.
- Conduct or facilitate vulnerability assessments of the sector.
- Encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

An old proverb states that "a chain is only as strong as its weakest link". In this sense, the "chain" terminology represents the nation's cyberspace critical infrastructure. The Defense Industrial Base consists of over 215,000 firms spread over 250 unique industries around the world. Cyber infrastructure security is typically left up to the private sector, with voluntary participation in vulnerability assessments [59].

System administrators, engineers, and programmers need to be responsible for assessing and mitigating the risks, and performing their roles responsibly and ensuring the CIA Triad is not broken [60]. Multi-layered cyber security mechanisms need to be in place so that if an adversary is able to penetrate one layer, the next layer may be the one to stop or delay the penetration. DIB partners need to ensure that cyber security is one of the top-funded IT items. IT professionals must keep their skills current with the technology [61]. Companies must provide the necessary finances for appropriate cyber security investments, including the training and certification of their IT staff.

If the United States' cyberspace were to come under attack, there is legal guidance [62] available for addressing the cyberspace attack. The Law of Information Conflict (LOIC) is the "composite of the peacetime regime of international law, the law of conflict management, and the law of armed conflict that regulates the conduct of all state activities in cyberspace" [63]. The LOIC documents the legal options available for

responding to the cyberspace attack based on the severity of the attack [64]. In the National Strategy to Secure Cyberspace, DoD is designated as the lead sector-specific agency for protecting the Defense Industrial Base critical infrastructure. DoD experiences daily attacks on its own networks, yet does not resort to mounting counter attacks.

The National Security Agency and the Department of Homeland Security (DHS) in support of the President's National Strategy to Secure Cyberspace, February 2003, jointly sponsor the Centers of Academic Excellence program. This program promotes higher Information Assurance education with the intent to grow a group of skilled professionals who can assist in addressing vulnerabilities in our nation's critical cyberspace infrastructure.

At this point in time, it is still being discussed as to what actions DoD should take to respond to a cyber attack on the nation's critical infrastructures. The Homeland Security Law Handbook discusses the conditions and steps involved for responding to cyberspace attacks on the nation's infrastructure. It is important to get these concepts documented clearly in DoD policy and doctrine, so that if and when a cyber attack does occur, DoD personnel will have the guidance necessary to respond strategically, tactically, and operationally. The National Military Strategy for Cyber Operations has been developed and is classified.

The DoD needs to continue working with the technology producers (hardware and software) for developing cyber security products that are the backbone of our nation's infrastructure [65]. DoD's role for protecting and defending the nation's Defense

Industrial Base critical infrastructure is complicated as the majority of the DIB is owned by the public sector, and is scattered around the world. The technology producers need to be aware that their responsible development and implementation of systems could be the difference between life and death for our DoD forces [60].

Holding the DIB accountable for developing and incorporating cyber security into those systems being used by DoD to accomplish its mission is not yet realized. The DIB is contractually held accountable for delivering products and services as written into the contracts. If cyber security is not written into the contract, then the nation cannot hold the DIB members accountable when the service or product has vulnerabilities able to be exploited by an adversary, thus increasing an adversary's information superiority over the United States.

5.2. Recommendations for Future Research

There are several areas for research that can assist the United States in securing its cyberspace: (1) Attributing cyberspace entity presence to physical location; and (2) Mandatory DIB critical infrastructure protection participation.

The first area of recommended future research discusses developing technology to attribute a user or adversary to a specific geo-physical location. Dr. Dorothy Denning and Professor Peter MacDoran discussed improving computer and network security by using a new form of location-based authentication which has the effect of grounding cyberspace to a physical location thereby helping to attribute attacks to a geo-physical location [66]. This geo-location-based authentication system would enforce authentication based on authorized physical location of individual, much like the concept

of calling from your home phone to activate a new credit card: the home phone number has to match the information in the company's database. This type of authentication system would provide the capability to track a user to a physical location.

The second area of recommended future research would encourage the Defense Contract Management Agency to add language to its contracts regarding cyber security of the products or services being delivered. The Defense Contract Management Agency (DCMA) is designated by DoD as the defense industrial base sector lead agent. DCMA performs worldwide acquisition life cycle contract management for Department of Defense weapon system programs, spares, supplies and services. This includes ensuring on-time delivery, at the right cost and in accordance with performance standards prescribed in over 360,000 contracts valued at over $900 billion with over 25,000 domestic and foreign contractors. DCMA information located on the DCMA website (www.dcma.mil) does not indicate they have updated the contractual language to reflect DCIP vulnerability assessments are required for DIB members doing business with the government or that cyber security needs to be implemented within the company and its services or products [67]. It appears that vulnerability assessments are purely voluntary. This is an area that should require vulnerability assessments and contractual language requiring cyber security be built into the company's IT systems, applicable products and services. On the flip side of the coin, it is in a DIB's best interests to be the company that implements cyber security into its services and products. No company wants to be the one with the headlines blaring "Company loses corporate and personal information to hacker, losses are estimated to be in millions" or "Company's IT system failure causes

loss of life on war field". Imagine the confidence level of the stockholders when that happens, affecting directly the economic well-being of the company.

5.3. Conclusion

DoD's role for securing United States cyberspace is to serve as the lead Sector Specific Agency (SSA) for the Defense Industrial Base (DIB). The DIB provides DoD with the capabilities (missiles, aircraft, troop support, space, combat vehicles, ammunition, weapons, information technology, shipbuilding, electronics, and mechanical, structural, electrical, and electronic parts) to perform its mission. These capabilities provide DoD with the products and services necessary to equip, inform, mobilize, deploy, and sustain operations worldwide. DoD relies on the DIB to meet requirements to fulfill the National Military Strategy.

It is voluntary for the DIB to work with DoD in performing critical infrastructure protection mission assurance assessments (CIP-MAA). The DIB is not obligated to comply with the CIP-MAA. DoD can make the DIB aware of potential threats, but it is up to the DIB to manage the risks by deterring the threats, mitigating the vulnerabilities, and minimizing the consequences. A risk assumed by one is a risk assumed by all.

If directed by the President or the SecDef of the United States, DoD can provide assistance to local law enforcement agencies, provide intelligence and information-sharing to assist in characterizing the cyber attack and attributing the attack to an entity, assist in law enforcement operations, and perform military operations to defend the homeland. DoD can take actions to deter or defend against cyber attacks which pose an imminent threat to national security based on applicable laws and policies.

DoD's challenge for securing the Defense Industrial Base critical infrastructure is to put processes in place to protect its cyberspace infrastructure by identifying and prioritizing critical assets and performing risk management [68]. Cyber security is all about the people, the processes, and the technology. Educating our people (users, managers, technicians, engineers, scientists, programmers) in their associated disciplines, improving on the processes for maintaining a secure cyberspace infrastructure, and improving the technology (building cyber security into hardware and software) contribute to improving cyberspace security. Cyberspace security cannot be achieved without all three of these factors (people, processes, and technology) taken into consideration. Information superiority cannot be achieved without cyber security.

The threats still exist for an adversary to physically attack the United States, but a skilled cyberspace adversary could strike at the heart of America's homeland with little cost, without ever leaving the comforts of home and retain anonymity. Our reliance on the power and capabilities of these ITs, which may contain vulnerabilities exploitable by an adversary, could ultimately be our weakness, our Achilles Heel.

Appendix A. Acronym List

9/11	11 September 2001
ASD	Assistant Secretary of Defense
CCDR	Combatant Commander
CIA	Confidentiality, Integrity, Availability
CI/KR	Critical Infrastructure and Key Resources
CJCS	Chairman of Joint Chiefs of Staff
CIP	Critical Infrastructure Protection
DCIP	Defense Critical Infrastructure Program
DCMA	Defense Contract Management Agency
DDOS	Distributed Denial of Service
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DIME	Diplomatic, Information, Military, and Economic
DII	Defense Information Infrastructure
DoD	Department of Defense
EO	Executive Order
F2T2EA	Find, Fix, Track, Target, Engage, Assess
GAO	Government Accountability Office
GIG	Global Information Grid
HSPD	Homeland Security Presidential Directive
IP	Internet Protocol

IS	Information Systems
IT	Information Technology
JCS	Joint Chiefs of Staff
JFCC-NW	Joint Functional Component Command – Network Warfare
JTF-GNO	Joint Task Force – Global Network Operations
MAA	Mission Assurance Assessment
NCA	National Command Authority
NDS	National Defense Strategy
NII	National Information Infrastructure
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NMS	National Military Strategy
NMS-CO	National Military Strategy for Cyber Operations
NORAD	North American Aerospace Defense
NPPD	National Protection and Programs Directorate
NRP	National Response Plan
NSA	National Security Agency
NSPD	National Security Presidential Directive
NSS	National Security Strategy
OBE	Overcome By Events
OODA	Observe, Orient, Decide, Act
OSD	Office of Secretary of Defense
SECDEF	Secretary of Defense

SSA	Sector Specific Agency
SSP	Sector Specific Plan
UC	Unified Command
U.S.	United States
US	United States
USC	United States Code
USCENTCOM	United States Central Command
USEUCOM	United States Europe Command
USJFCOM	United States Joint Forces Command
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
USSOUTHCOM	United States South Command
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command
VOIP	Voice Over Internet Protocol

Appendix B. Terms and Definitions

Achilles Heel - a fatal weakness that leads or may lead to a downfall. (Cyber Warfare and Cyber Terrorism, pg 33).

Asset (Infrastructure) - A distinguishable network entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and owned or operated by domestic, foreign, public, or private sector organizations. (DoDD 3020.40)

Botnet - A network of remote-controlled zombie computers. Using Trojan Horse programs or worms/viruses, a person (often called a "botmaster" or "herder") can inject malware into a user's computer which opens a port to listen for commands; often via an internet relay chat (IRC) channel. When the commands are received then the zombie computer (as they are called) executes its instructions which often involve sending out massive amounts of spam, copies of other malware, or popup advertising. The user of the zombie may not even be aware this is happening unless they notice a slowdown of their computer or a large amount of Internet activity. (Computer Knowledge)

Characterization (Infrastructure) - The analytic decomposition of functions, systems, assets, and dependencies as they relate to supporting DoD operational capabilities and assets. (DoDD 3020.40)

CIA Triad – An information security model that requires that these three key principles be implemented to secure systems: Confidentiality, Integrity, and Availability. Confidentiality prevents unauthorized disclosure of sensitive information. Integrity ensures that data is an accurate and unchanged representation of the original secured information. Availability is having reliable and timely access to the data and resources you are authorized to use. (CISSP)

Critical Asset - A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. (JP3-07.2)

Critical Infrastructure – Assets, systems and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (NIPP)

Critical Infrastructure Protection - Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include: changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc. (JP3-28)

Cybersecurity – See Information Security.

Cyberspace – a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated infrastructures. (NMS-CO)

Cyberspace - the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. (NSPD-54/HSPD-23)

Cyber Storm Exercise - The National Cyber Exercise (NCE) Cyber Storm was executed successfully on February 6–10, 2006. The United States (U.S.) Department of Homeland Security (DHS)/National Cyber Security Division (NCSD) was responsible for developing, implementing, and coordinating all aspects of Cyber Storm. The first Government-led, full-scale, cyber security exercise of its kind, Cyber Storm was a coordinated effort between international, Federal and State governments, and private sector organizations to exercise their response, coordination, and recovery mechanisms in reaction to simulated cyber events. Cyber Storm provided participants with a controlled environment in which to exercise a coordinated cyber incident response, including information sharing mechanisms, procedures for establishing situational awareness, public and private organizational decision making, and public communications during a cyber-related Incident of National Significance. Over 100 public and private agencies, associations, and corporations participated in the exercise from over 60 locations and 5 countries. They collaborated in crisis response at operational, policy and public affairs levels in this federally funded and congressionally mandated emergency response exercise. The exercise included participation of more than 30 private sector corporations and associations in its planning, execution, and after action analysis. The exercise scenario simulated a large-scale cyber campaign affecting or disrupting multiple critical infrastructure elements primarily within the Energy, Information Technology, Transportation, and Telecommunications Sectors. The exercise was conducted primarily on a separate exercise network without impacting real world information systems. (DHS Cyber Storm Exercise Report – September 2006)

Defense Critical Asset - An asset of such extraordinary importance to DoD operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its missions. (DoDD 3020.40)

Defense Critical Infrastructure - DoD and non-DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide. (DoDD 3020.40)

Defense Critical Infrastructure - the DOD and non-DOD networked assets essential to project, support, and sustain military forces and operations worldwide. Assets are people, physical entities, or information. Physical assets would include installations, facilities, ports, bridges, power stations, telecommunication lines, pipelines, etc. The increasing

interconnectivity and interdependence among commercial and defense infrastructures demand that DOD take steps to understand and remedy or mitigate the vulnerabilities of, and threats to, the critical infrastructures on which it depends for mission accomplishment. (JP3-27)

Defense Critical Infrastructure Program (DCIP) - A DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy. (DoDD 3020.40)

Defense Critical Infrastructure Program (DCIP) - The DCIP is a fully integrated program that provides a comprehensive process for understanding and protecting selected infrastructure assets that are critical to national security during peace, crisis, and war. It involves identifying, prioritizing, assessing, protecting, monitoring, and assuring the reliability and availability of mission-critical infrastructures essential to the execution of the NMS. The program also addresses the operational decision support necessary for CCDRs to achieve their mission objectives despite the degradation or absence of these infrastructures. (JP3-27)

Defense Industrial Base (DIB) - The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. (JP 3-27)

Defense Industrial Base (DIB) Defense Sector - The Department of Defense, the U.S. Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. (DIB-SSP)

Defense Information Infrastructure - The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving Department of Defense (DOD) local, national, and worldwide information needs. The defense information infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecom-munications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information. Also called DII. (JP 3-13)

Defense Information Systems Network - Integrated network, centrally managed and configured to provide long-haul information transfer services for all Department of Defense activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services. Also called DISN. (JP 2-01)

Defense Sector - A virtual association within the DCIP that traverses normal organizational boundaries, encompasses defense networks, assets, and associated dependencies,that perform similar functions within the Department of Defense and are essential to the execution of the National Military Strategy. (DoDD 3020.40)

Defense Support of Civil Authorities — Civil support provided under the auspices of the National Response Plan. Also called DSCA. (JP 3-28)

Defense support of civil authorities – often referred to as civil support, is DoD support, including Federal military forces, the Department's career civilian and contractor personnel, and DoD agency and component assets, for domestic emergencies and for designated law enforcement and other activities. The Department of Defense provides defense support of civil authorities when directed to do so by the President or Secretary of Defense. (DoD Strategy for Homeland Defense and Civil Support)

Department of Defense components - The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Department of Defense agencies, field activities, and all other organizational entities in the Department of Defense. (JP 1)

Dependency - A relationship or connection whereby one entity is influenced or controlled by another entity. (Dodd 3020.40)

Diplomatic, Information, Military and Economic (DIME) - Areas of national power that are leveraged in "effects-based" operations against an adversary's vulnerabilities identified by Operational Net Assessment, and targeted against his will and capability to conduct war. (USJFCOM Glossary)

Distributed Denial of Service - An attack sent by an individual or individuals which can be set up to be sent automatically by programs known as Zombies that may have been installed in various computers in advance of the attack. With Zombies, all the attacker need do is send a single command and they perform the attack. This method can more easily isolate the attacker from those who might want to find him/her as the attack itself is coming from completely unrelated computers that may be half a world away. These DDoS attacks may even use your computer through a zombie installed by a worm. (Computer Knowledge)

Electromagnetic Spectrum - The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP1-02)
Emergency Response Providers - includes Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.

Financial Services Defense Sector - The DoD, government, and private sector worldwide network and its supporting infrastructure that meet the financial services needs of DoD users across the range of military operations. (DoDD 3020.40)

Global Information Grid - The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. Also called GIG. (JP 6-0)

Global Information Grid (GIG) Defense Sector - The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel including all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in Section 5142 of the Clinger-Cohen Act of 1996 (reference (g)). (DoDD 3020.40)

Global Information Infrastructure - The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. Also called GII. (JP 3-13)

Global Positioning System - A satellite constellation that provides highly accurate position,velocity, and time navigation information to users. Also called GPS. (JP1-02)

Hazard (Infrastructure) - Non-hostile incidents such as accidents, natural forces, technological failure, etc., that cause loss or damage to infrastructure assets. (DoDD 3020.40)

Health Affairs Defense Sector - The DoD, government and private sector worldwide health care network and its supporting infrastructure that meet the health care needs of DoD users across the range of military operations. (DoDD 3020.40)

Homeland — The physical region that includes the continental United States, Alaska, Hawaii, United States possessions and territories, and surrounding territorial waters and airspace. (JP 3-28)

Homeland Defense — The protection of United States sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression or other threats as directed by the President. The DoD is responsible for Homeland Defense. Also called HD. (JP 3-27)

Information - 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 3-13.1)

Information Management — The function of managing an organization's information resources by the handling of knowledge acquired by one or many different individuals and organizations in a way that optimizes access by all who have a share in that knowledge or a right to that knowledge. (JP 3-0)

Information Operations — The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. Also called IO. (JP 3-13)

Information Security — The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Also called INFOSEC. (JP 3-13)

Information Superiority — The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 3-13)

Information System — The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (JP 3-13)

Infrastructure - The framework of networked assets that comprise identifiable industries, institutions, or distribution capabilities that enable a continued flow of goods and services. (DoDD 3020.40)

Installation Preparedness. - The integration of key activities on DoD installations and facilities that address all efforts pertaining to prevention, detection, protection, response, and remediation against all threats and hazards. (DoDD 3020.40)

Intelligence, Surveillance, and Reconnaissance (ISR) Defense Sector - The DoD, government and private sector worldwide facilities, networks, and systems that conduct and support the collection, production, and dissemination of intelligence, surveillance and

reconnaissance information, in support of activities that meet the needs of DoD users across the range of military operations. (DoDD 3020.40)

Inter-Dependency - Relationships or connections between entities of different functions, networks, sectors, or services. (DoDD 3020.40)

Intra-Dependency - Relationships or connections between entities within a common function, network, sector, or service. (DoDD 3020.40)

Local Government - any county, city, village, town, district, or other political subdivision of any state, any Native American tribe or authorized tribal organization, or Alaska native village or organization, and includes any rural community or unincorporated town or village or any other public entity for which an application for assistance is made by a state or political subdivision thereof. (National Strategy for Homeland Security)

Logistics Defense Sector. The DoD, government, and private sector worldwide facilities, networks, and systems that support the provision of supplies and services to U.S. forces. (DoDD 3020.40)

Military Support to Civil Authorities — A mission of civil support consisting of support for natural or man-made disasters, chemical, biological, radiological, nuclear, or high-yield explosive consequence management, and other support as required. Also called MSCA. (DODD 3025.1)

Military Support to Civilian Law Enforcement Agencies — A mission of civil support that includes support to civilian law enforcement agencies. This includes but is not limited to: combating terrorism, counterdrug operations, national security special events, and national critical infrastructure and key asset protection. Also called MSCLEA. (DODD 3025.1)

Mission Assurance - A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy. It links numerous risk management program activities and security related functions—such as force protection; antiterrorism; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness—to create the synergistic effect required for DoD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations. (DoDD 3020.40)

Mitigation - Actions taken in response to a warning or after an incident occurs that are intended to lessen the potentially adverse effects on a given military operation or infrastructure. (DoDD 3020.40)

Monitoring and Reporting - The collection, fusion, and dissemination of intelligence based indications and warning, DoD asset and civil infrastructure readiness reporting, law enforcement information, man-made or natural hazards, and suspicious security event reporting, that can adversely impact mission readiness. (DoDD 3020.40)

National Command Authority - The President of the United States or the Secretary of Defense ability to exercise authority and control of the Armed Forces. (JP-1)

National Critical Infrastructure and Key Assets — The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. They include telecommunications, electrical power systems, gas and oil distribution and storage, water supply systems, banking and finance, transportation, emergency services, industrial assets, information systems, and continuity of government operations. Also called NCI&KA. (JP 3-28)

National Defense Strategy — A document approved by the Secretary of Defense for applying the Armed Forces of the United States in coordination with Department of Defense agencies and other instruments of national power to achieve national security strategy objectives. Also called NDS. (JP 3-0)

National Emergency — A condition declared by the President or the Congress by virtue of powers previously vested in them that authorize certain emergency actions to be undertaken in the national interest. Action to be taken may include partial, full, or total mobilization of national resources. (JP 3-28)

National Incident Management System — A national crisis response system that provides a consistent, nationwide approach for Federal, state, local, and tribal governments; the private sector; and nongovernmental organizations to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. Also called NIMS. (JP 3-41)

National Information Infrastructure — The nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure. Also called NII. (JP 3-13)

National Military Strategy — A document approved by the Chairman of the Joint Chiefs of Staff for distributing and applying military power to attain national security strategy and national defense strategy objectives. Also called NMS. (JP 3-0)

National Operations Center — The primary national hub for domestic incident management operational coordination and situational awareness. A standing 24 hours a day, 7 days a week interagency organization fusing law enforcement, national intelligence, emergency response, and private-sector reporting. Also called NOC. (JP 3-28)

National Response Coordination Center — A multiagency center that provides overall federal response and recovery coordination for incidents of national significance and emergency management program implementation. This center is a functional component of the national operations center. Also called NRCC. (JP 3-28)

National Security — A collective term encompassing both national defense and foreign relations of the United States. Specifically, the condition provided by: a. a military or defense advantage over any foreign nation or group of nations; b. a favorable foreign relations position; or c. a defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert. (JP1-02)

National Security Council — A governmental body specifically designed to assist the President in integrating all spheres of national security policy. The President, Vice President, Secretary of State, and Secretary of Defense are statutory members. The Chairman of the Joint Chiefs of Staff; Director, Central Intelligence Agency; and the Assistant to the President for National Security Affairs serve as advisers. Also called NSC. (JP1-02)

National Security Interests — The foundation for the development of valid national objectives that define US goals or purposes. National security interests include preserving US political identity, framework, and institutions; fostering economic well-being; and bolstering international order supporting the vital interests of the United States and its allies. (JP1-02)

National Security Strategy - A document approved by the President of the United States for developing, applying, and coordinating the instruments of national power to achieve objectives that contribute to national security. Also called NSS. (JP 3-0)

Network - A group or system of interconnected or cooperating entities, normally characterized as being nodes (assets) and the connections that link them. (DoDD 3020.40)

North American Aerospace Defense Command — A bi-national command of the US and Canada that provides aerospace surveillance, warning and assessment of aerospace attack, and maintains the sovereignty of US and Canadian airspace. Also called NORAD. (JP1-02)

Operational Net Assessment (ONA) - A continuously updated operational support tool that provides a JTF commander visibility of effects-to-task linkages based on a "system-

of-systems" analysis of a potential adversary's political, military, economic, social, infrastructure, and information (PMESII) war-making capabilities. The ONA informs decision-makers from strategic to tactical levels regarding the complementary effects and supporting missions and tasks that can be considered when applying the full range of diplomatic, information, military and economic (DIME) actions to achieve specific effects on an adversary's will and capability in support of national objectives. ONA is a critical enabler for achieving rapid decisive operations. It is an integrated, collaborative product of Department of Defense and other appropriate government and non-government organizations. Its purpose is to identify key links and nodes within the adversary's systems and to propose methods that will influence, neutralize or destroy them and achieve a desired effect or outcome. (USJFCOM Glossary)

Personnel Defense Sector - The DoD, government, and private sector worldwide network that coordinates and supports personnel and human resource functions of DoD personnel. (DoDD 3020.40)

Posse Comitatus Act — Prohibits search, seizure, or arrest powers to US military personnel. Amended in 1981 under Public Law 97-86 to permit increased Department of Defense support of drug interdiction and other law enforcement activities. (Title 18, “Use of Army and Air Force as Posse Comitatus” - United States Code, Section 1385) (JP1-02)

Protect – reducing the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks.

Public Works Defense Sector - The DoD, government, and private sector worldwide network, including the real property inventories (environment, land, buildings, and utilities), that manages the support, generation, production, and transport of commodities (e.g., electric power, oil and natural gas, water and sewer, emergency services, etc.) for and to DoD users. (DoDD 3020.40)

Remediation - Actions taken to correct known deficiencies and weaknesses. These actions are undertaken once a vulnerability has been identified. (DoDD 3020.40)

Reserve Components - Reserve Components of the Armed Forces of the United States are: a.the Army National Guard of the United States; b. the Army Reserve; c. the Naval Reserve; d. the Marine Corps Reserve; e. the Air National Guard of the United States; f. the Air Force Reserve; and g. the Coast Guard Reserve. Also called RCs. (JP 4-05)

Risk - Probability and severity of loss linked to threats or hazards. (DoDD 3020.40)

Risk Assessment – is a systematic examination of risk, using disciplined processes, methods, and tools. It provides an environment for decision making to continuously evaluate and prioritize risks and recommend strategies to remediate or mitigate those risks. (DoDD 3020.40)

Risk Management - A process by which decision makers accept, reduce, or offset risk. (DoDD 3020.40)

Sector-Specific Agency – federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category.

Secure – reducing the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks.

Space Defense Sector - The DoD, government, and private sector worldwide network, including both space- and ground-based systems and facilities, that supports launch, operation, maintenance, specialized logistics, control systems, etc., for DoD users.

State - any state of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Canal Zone, the Commonwealth of the Northern Mariana Islands, or the trust territory of the Pacific Islands. (National Strategy for Homeland Security)

Strategy - A prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives. (JP 3-0)

Theater Strategy - Concepts and courses of action directed toward securing the objectives of national and multinational policies and strategies through the synchronized and integrated employment of military forces and other instruments of national power. (JP 3-0)

Threat - An adversary having the intent, capability, and opportunity to cause loss or damage. (DoDD 3020.40)

Transportation Defense Sector - The DoD, government, and private sector worldwide network that provides U.S. military lift support (surface, sea, and air) for military operations. (DoDD 3020.40)

Vulnerability (Infrastructure) - The characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard. (DoDD 3020.40)

Vulnerability Assessment (Infrastructure) - A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities. (DoDD 3020.40)

Bibliography

1. Greenemeier, Larry. "Estonian 'Cyber Riot' Was Planned, But Mastermind Still A Mystery," Information Week, 3 August 2007. http://www.informationweek.com/security/showArticle.jhtml?articleID=201202784. Accessed 6 February 2008.

2. Computer Knowledge. "Botnet," 11 March 2006. http://www.cknow.com/ckinfo/b/Botnet-Anetworkofremote-c.html. Accessed 1 June 2007

3. Landler, Mark and Markoff, John. "Digital Fears Emerge After Data Siege in Estonia," New York Times, 29 May 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html. Accessed 1 June 2007.

4. Claburn, Thomas. "Estonian Hacker Fined For Cyber Attack," Information Week, 25 January 2008. http://www.informationweek.com/security/showArticle.jhtml?articleID=205918839. Accessed 6 February 2008.

5. Internet World Stats Usage and Population Statistics. 30 November 2007. Estonia. http://www.internetworldstats.com/stats9.htm#eu. Accessed 23 January 2008.

6. Internet World Stats Usage and Population Statistics. 30 November 2007. United States. http://www.internetworldstats.com/stats14.htm#north. Accessed 23 January 2008.

7. Rice, Condoleeza. Remarks by Condoleeza Rice at Partnership For Critical Infrastructure Annual Meeting. Washington, D.C. 22 March 2001.

8. Kass, Lani Dr. "Cyberspace: A Warfighting Domain," HQ USAF, AF Cyberspace Task Force, 26 September 2006.http://www.afa.org/media/scripts/ppt_pdf/AFACyberspaceTaskForceBrief.pdf Accessed 6 February 2008.

9. United States House of Representatives. *A Failure of Initiative Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina.* 15 February 2006. Washington D.C.: Government Printing Office, 2006. http://www.gpoaccess.gov/katrinareport/mainreport.pdf. Accessed 7 January 2008.

10. Department of Defense. *National Military Strategy for Cyber Operations (NMS-CO).* Washington D.C.: Government Printing Office, 2007.

11. Colonels Qiao Liang and Wang Xiangsui, Peoples Liberation Army (PLA). Chinese IW Doctrine "Unrestricted Warfare", February 1999.

12. The White House. National Security Act of 1947, http://www.whitehouse.gov/nsc/. (Accessed 28 November 2007)

13. The White House. Executive Order 13231 – Critical Information Protection in Information Age, October 2001. http://www.whitehouse.gov/nsc/. (Accessed 28 November 2007)

14. United States Code Title 50 - War and National Defense. http://uscode.house.gov/download/title_50.shtml (Accessed 28 November 2007)

15. The White House. *The National Strategy for Homeland Security.* Washington D.C.: Government Printing Office, 2002.

16. The White House. *Homeland Security Act of 2002.* Washington D.C.: Government Printing Office, 2002.

17. The White House. *HSPD-5 Management of Domestic Incidents*. Washington D.C.: Government Printing Office, 2003.

18. The White House. *The National Strategy to Secure Cyberspace.* Washington D.C.: Government Printing Office, 2003.

19. The White House. *National Strategy for Homeland Security.* Washington D.C.: Government Printing Office, 2002.

20. The White House. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Washington D.C.: Government Printing Office, 2003.

21. The White House. *HSPD-7 Critical Infrastructure Identification, Prioritization, and Protection.* Washington D.C.: Government Printing Office, 2003.

22. The White House. *The National Military Strategy of the United States of America.* Washington D.C.: Government Printing Office, 2004.

23. Department of Homeland Security. *National Response Plan*. Washington D.C.: Government Printing Office, 2004.

24. The White House. *The National Defense Strategy of the United States of America.* Washington D.C.: Government Printing Office, 2005.

25. Department of Defense. *Strategy for Homeland Defense and Civil Support.* Washington D.C.: Government Printing Office, 2005.

26. Department of Defense. *DoD Directive 3020.40 Defense Critical Infrastructure Program.* Washington D.C.: Government Printing Office, 2005.

27. The White House. *The National Security Strategy of the United States of America*. Washington D.C.: Government Printing Office, 2006.

28. Department of Homeland Security. *The National Infrastructure Protection Plan.* Washington D.C.: Government Printing Office, 2006.

29. Department of Homeland Security and Department of Defense. *Defense Industrial Base Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan.* Washington D.C.: Government Printing Office, 2007.

30. Department of Defense. *Joint Publication 1, Doctrine for the Armed Forces of the United States (JP1).* Washington D.C.: Government Printing Office, 2007. pxiv.

31. Department of Defense. *Joint Publication 3-27, Homeland Security (JP3-27).* Washington D.C.: Government Printing Office, 2007.

32. Department of Homeland Security. DHS Organization Chart. www.dhs.gov/xlibrary/assets/DHS_OrgChart.pdf. Accessed 23 January 2008.

33. Shanor, Charles A. and Hogue, L. Lynn. National Security and Military Law. Thomson West, 2003.

34. The White House. *President Bush's Letter to the American People for The National Strategy to Secure Cyberspace.* Washington D.C.: Government Printing Office, 2003.

35. Department of Homeland Security. *National Response Plan, Cyber Incident Annex.* Washington D.C.: Government Printing Office, 2004.

36. United States Government Accountability Office. *"Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DoD's Risk Management Approach for the Defense Industrial Base."* GAO-07-1077. Washington D.C. August 2007. www.gao.gov/cgi-bin/getrpt?GAO-07-1077. Accessed 6 February 2008.

37. Department of Defense. *Joint Publication 3-28, Civil Support (JP3-28).* Washington D.C.: Government Printing Office, 2007.

38. United States Strategic Command. USSTRATCOM Mission Statement. http://www.stratcom.mil/ Accessed 7 January 2008.

39. United States Strategic Command. JTF-GNO Mission Statement. http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html Accessed 7 January 2008.

40. United States Strategic Command. USSTRATCOM Functional Components. http://www.stratcom.mil/organization-fnc_comp.html Accessed 7 January 2008.

41. United States Code Title - 10 Armed Forces. http://www.access.gpo.gov/uscode/title10/title10.html (Accessed 27 November 2007)

42. United States Code Title 32 - National Guard. http://www.access.gpo.gov/uscode/title32/title32.html (Accessed 27 November 2007)

43. Posner, Michael. "America Already is in a Cyber War, Analyst Says," National Journal's Technology Daily. 27 November 2007. http://www.govexec.com/ story_page.cfm?articleid=38667. Accessed 6 February 2008.

44. The CIP Report. "*Defense Industrial Base*." Critical Infrastructure Protection Program, Volume 5 Number 8. George Mason University, School of Law. Zeichner Risk Analytics, LLC (ZRA). February 2007.

45. Howard, John D. "An Analysis Of Security Incidents On The Internet," Carnegie Mellon University Thesis April 7, 1997. http://www.cert.org/research/JHThesis/ Accessed 1 October 2007.

46. The White House. *Inaugural Address of President John F. Kennedy, 20 January 1961*. http://www.jfklibrary.org/Historical+Resources/Archives/Reference+Desk/ Speeches/JFK/003POF03Inaugural01201961.htm Accessed 7 January 2008.

47. Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos. "Digital crime and Forensic Science." Idea Group Publishing, 2006. Pg 244

48. Kurose, Jim and Ross, Keith. "Computer Networking: A Top Down Approach Featuring the Internet, 3rd edition." Addison-Wesley, July 2004.

49. Bishop, Matt. "Computer Security: Art and Science." Addison-Wesley, 2002.

50. ABS Consulting. Homeland Security Law Handbook. Government Institutes, 2003.

51. Weiner, Norbert. Cybernetics: or Control and Communication in the Animal and the Machine. Cambridge, MA: MIT Press. 1948

52. Conway, Flo and Siegelman, Jim. "Dark Hero Of The Information Age: In Search Of Norbert Weiner The Father Of Cybernetics." Basic Books, 2004. pp171-194.

53. Department of Homeland Security. *Cyber Storm Exercise Report*. Washington D.C.: Government Printing Office, 2006.

54. Department of Homeland Security. *Cyber Storm II National Cyber Exercise for March 2008*. Washington D.C.: Government Printing Office, 2007.

55. Report for Congress. The Economic Effects of 9/11: A Retrospective Assessment. Washington D.C.: Government Printing Office, 2002.

56. Whoriskey, Peter. Biloxi's Recovery Shows Divide While Casinos Prosper, Katrina's Mark Lingers in Working-Class Areas. Washington Post, 25 November 2007; Page A03. http://www.washingtonpost.com/wp-dyn/content/article/2007/11/24/AR2007112400616.html?sub=AR (Accessed 7 February 2008)

57. The CIP Report. "*Defense Industrial Base*." Critical Infrastructure Protection Program, Volume 5 Number 8. George Mason University, School of Law. Zeichner Risk Analytics, LLC (ZRA). February 2007.

58. Thomas, Timothy L. Dragon Bytes: Chinese Information – War Theory and Practice from 1995 – 2003. Foreign Military Studies Office: Fort Leavenworth, KS, 2004. Pg-87.

59. ABS Consulting. Homeland Security Law Handbook. Government Institutes, 2003.

60. Baase, Sara. A Gift of Fire: Social, Legal, and Ethical Issues for Computers and the Internet, 2nd edition. Prentice Hall, 2003.

61. Galliers, Robert D. and Leidner, Dorothy E. Strategic Information Management: Challenges and Strategies in Managing Information Systems, third edition. Elsevier Butterworth-Heinemann, 2003.

62. Wingfield, Thomas C. The Law of Information Conflict: National Security Law in Cyberspace. Aegis Research Corporation, 2000a.

63. Wingfield, Thomas C. The Law of Information Conflict: National Security Law in Cyberspace. Aegis Research Corporation, 2000a. pp10-11

64. Wingfield, Thomas C. The Law of Information Conflict: National Security Law in Cyberspace. Aegis Research Corporation, 2000b. pp123-129

65. Rattray, Greg. Strategic Warfare in Cyberspace. Cambridge, MA: MIT Press 2001. pp 461-480.

66. Denning, Dorothy E. and Denning, Peter J. Internet Besieged: Countering Cyberspace Scofflaws. Addison-Wesley, 1998. pp167-174.

67. Defense Contract Management Agency. http://www.dcma.mil/aboutDCMA.htm Accessed on 7 Jan 2008.

68. Kanellis, Panagiotis and Kiountouzis, Evangelos and Kolokotronis, Nicholas and Martakos, Drakoulis. "Digital Crime and Forensic Science." Idea Group Publishing, 2006.

Additional Materials Reviewed But Not Referenced

ASD-NII/CIO. ASD-NII/CIO. http://www.defenselink.mil/cio-nii/ Accessed 10 February 2008.

Col John A. Warden III, "Air Theory for the Twenty-first Century", Battlefield of the Future, 21st Century Warfare Issues, September 1995, http://www.airpower.maxwell.af.mil/airchronicles/battle/chp4.html (accessed 1 June 07)

Denise Pappalardo. "Top 10 IT Priorities at the DoD", 13 April 2007, Network World, www.networkworld.com/news/2007/041307-it-priorities-dod.html. (Accessed 4 December 2007)

Department of Defense. *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms (JP1-02).* Washington D.C.: Government Printing Office, 2007.

Department of Defense. *Joint Publication 3-0, Joint Operations (JP3-0).* Washington D.C.: Government Printing Office, 2006.

Department of Defense. *Joint Publication 3-13, Information Operations (JP3-13).* Washington D.C.: Government Printing Office, 2006.

Department of Defense. *Joint Publication 3-13.1, Electronic Warfare (JP3-13.1).* Washington D.C.: Government Printing Office, 2007.

Department of Defense. *Joint Publication 3-26, Homeland Security (JP3-26).* Washington D.C.: Government Printing Office, 2005.

Department of Defense. *Joint Publication 3-41, Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management (JP3-41).* Washington D.C.: Government Printing Office, 2006.

Department of Defense. *Joint Publication 4-05, Joint Mobilization Planning (JP4-05).* Washington D.C.: Government Printing Office, 2006.

Department of Defense. *Joint Publication 4-05.1, Joint Tactics, Techniques, and Procedures for Manpower Mobilization and Demobilization Operations: Reserve Component (RC) Callup (JP4-05.1).* Washington D.C.: Government Printing Office, 1998.

Department of Defense. *Joint Publication 6-0, Joint Communications System (JP6-0).* Washington D.C.: Government Printing Office, 2006.

Department of Defense. *DoD Directive 5100.20 The National Security Agency and the Central Security Service.* Washington D.C.: Government Printing Office, 1991.

Department of Defense. *DoD Directive 5105.19 Defense Information Systems Agency.* Washington D.C.: Government Printing Office, 2006.

Department of Defense. *DoD Directive 5144.1 Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO).* Washington D.C.: Government Printing Office, 2005.

Department of the Air Force. "Compliance with the Law of Armed Conflict". Air Force Policy Directive (AFPD) 51-4.Washington:HQ USAF. 26 April 1993.

Lawrence Berkeley National Laboratory, "The Electromagnetic Spectrum," http://www.lbl.gov/MicroWorlds/ALSTool/EMSpec/EMSpec2.html (accessed 1 June 2007).

Lt Gen Bob Elder, Commander, 8AF, "Air Force Cyber Operations Command Mission: Warfighting", 5 January 2007.

Major Gary Cornn, "Cyberspace: Mission and Challenges", 2 October 2006, AF Cybertask Force (accessed May 2007)

MSgt Mitch Gettle, "Air Force Releases New Mission Statement," Air Force Print News, 8 December 2005, Air Force Link, http://www.af.mil/news/story.asp?id= 123013440 Accessed 1 May 2007

SSgt C. Todd Lopez, "8th Air Force To Become New Cyber Command," Air Force Print News, 3 November 2006, Air Force Link, http://www.af.mil/news/story.asp?id =123030505 Accessed 1 May 2007

SSgt C. Todd Lopez, "Fighting in Cyberspace Means Cyber Dominance," Air Force Print News, 28 February 2007, Air Force Link, http://www.af.mil/news/story.asp?id= 123042670 (accessed 1 May 2007).

United States Department of Homeland Security, "Portfolios: Critical Infrastructure Protection," 6 September 2006, http://www.dhs.gov/xres/programs/editorial_0548.shtm (accessed 24 May 2007).

White House. NSPD-54/HSPD-23. Washington D.C.: Government Printing Office, 2008.

Winther, Mark. "White Paper Tier 1 ISPs: What They Are and Why They Are Important," IDC, May 2006, Sponsored by NTT Communications, http://www.ntt.net/english/library/pdf/IDCTier1-Whitepaper.pdf (accessed 1 May 2007).

Vita

Mrs. Jane Griffin graduated from Meigs High School located in Pomeroy, Ohio in 1973. Jane enlisted in the United States Navy (USN) and served on active duty from October 1973 to February 1981. Jane separated from the USN with an Honorable Discharge as a First Class Petty-Officer (E-6) Data Systems Technician in Philadelphia, PA. Jane completed an Associate in Applied Science (AAS) in Data Processing and graduated from Delaware County Community College Media, PA in January 1982. She then worked as a computer programmer from January 1982 to January 1985 at Computer Sciences Corporation (CSC) in Moorestown, NJ, maintaining and developing software for use aboard USN AEGIS-class ships.

While working full-time, Jane attended Saint Joseph's University evening college in Philadelphia, PA and completed a Bachelor of Science (BS) in Information Systems in May 1984. Jane resigned her position with CSC in January 1985 in order to attend Saint Joseph's University graduate school full-time. She completed a Master in Business Administration (MBA) with an emphasis on Information Systems in May 1986.

Jane returned to Ohio the summer of 1986. Jane accepted a computer programming position at Sinclair Community College in January 1987, resigning her position in February 1988 to advance her career at SofTech, Inc. Note: SofTech, Inc. was acquired by CACI, Inc in ~1995. Jane worked as a computer programmer on several USN projects from February 1988 to June 1998 and performed Independent Verification and Validation (IV&V) Year 2000 (Y2K) testing of United States Air Force applications from June 1998 to January 2000. Jane resigned in January 2000 from CACI, Inc to

accept a civil service position with the National Air & Space Intelligence Center (NASIC) at WPAFB to perform Information Assurance duties.

Jane has worked at NASIC since January 2000. In June 2006, Jane was selected by the National Security Agency (NSA) Department of Defense (DoD) Information Assurance scholarship program to attend Air Force Institute of Technology (AFIT) to complete an 18-month Master of Science (MS) program in Cyber Operations from September 2006 to March 2008.

Upon graduating from AFIT, Jane returned to NASIC with the intent to further grow the existing Information Assurance Office.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
27-03-2008	Master's Thesis	October 2007 – March 2008

4. TITLE AND SUBTITLE

DOD ROLE FOR SECURING UNITED STATES CYBERSPACE

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Griffin, Jane J., GG-13, DAF

5d. PROJECT NUMBER
JON # 08-159

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GCO/ENG/08-03

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Mr. Robert Kaufman
Director, Information Operations
AFIOC/IO
Lackland AFB, TX 78243-7038
email: robert.kaufman@lackland.af.mil phone: DSN 969-5377

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The cyber attacks on Estonia in late April and the early weeks of May 2007 significantly crippled the country, preventing it from performing banking, communications, news reporting, government transactions and command and control activities. Estonia is considered a "Wired Society", much like the United States. Both countries rely on the cyberspace infrastructure economically and politically. Estonia sought assistance outside the country to recover from and to address the attacks. The cyber attacks on Estonia focused world-wide attention on the effects that cyberspace attacks could have on countries. If a cyber attack of national significance occurred against the United States, what would the United States do? The Department of Defense is responsible for protecting the nation and its geographical boundaries from attack, but what is DoD's role for securing the United States' cyberspace? Research was conducted by studying national orders, strategies, policies plans, and doctrine to determine DoD's role for securing the United States' cyberspace. Research revealed that DoD is assigned the lead role as Sector Specific Agency (SSA) for the Defense Industrial Base (DIB). As the lead SSA for the DIB, DoD's role for securing the United States' cyberspace is to identify, assess, and improve risk management of the critical infrastructure within the DIB. Our nation's defense and military strength rely on the DoD which in turn relies on the DIB to enable DoD to perform its mission. Participation by the DIB is on a voluntary basis, with DIB participants making the risk management calls and implementing the strategies that best fit their needs, which may not serve national security objectives.

15. SUBJECT TERMS

Defense Industrial Base, Securing United States Cyberspace, Cyber Storm Exercise, Risk Management, DIB, Critical Infrastructure, Critical Infrastructure Protection Mission Assurance Assessment, DCIP, DoD Role

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Robert F. Mills, PhD
U	U	U	UU	98	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 4527 (robert.mills@afit.edu)